



# Aplicación Citrix Workspace para iOS

## Contents

<b>Aplicación Citrix Workspace para iOS</b>	<b>2</b>
<b>Acerca de esta versión</b>	<b>3</b>
<b>Funciones en Technical Preview</b>	<b>32</b>
<b>Requisitos del sistema y compatibilidad</b>	<b>56</b>
<b>Instalación y actualización</b>	<b>64</b>
<b>Introducción</b>	<b>64</b>
<b>Configurar la aplicación Citrix Workspace</b>	<b>73</b>
<b>Configurar la aplicación Workspace mediante soluciones de administración unificada de dispositivos de punto final</b>	<b>85</b>
<b>Dispositivos periféricos</b>	<b>88</b>
<b>Experiencia de usuario</b>	<b>110</b>
<b>Vista web para aplicaciones web y SaaS</b>	<b>121</b>
<b>Administración de contraseñas</b>	<b>122</b>
<b>Autenticación</b>	<b>126</b>
<b>Protección</b>	<b>152</b>
<b>Solucionar problemas técnicos</b>	<b>158</b>
<b>Aplicación Citrix Workspace para iOS</b>	<b>170</b>

## Aplicación Citrix Workspace para iOS

July 1, 2024

El software de cliente de la aplicación Citrix Workspace para iOS está disponible para su descarga desde el App Store. Le permite acceder a aplicaciones y ejecutar escritorios alojados, entregados por Citrix Virtual Apps and Desktops.

iOS es el sistema operativo de los dispositivos móviles de Apple, como iPads y iPhones. La aplicación Citrix Workspace para iOS se ejecuta en dispositivos que usan el sistema operativo iOS, por ejemplo iPhone X, iPad mini y iPad Pro.

Para obtener información detallada sobre funciones, problemas resueltos y problemas conocidos, consulte la página [Acerca de esta versión](#).

Para obtener información sobre los elementos retirados, consulte la página [Elementos retirados](#).

### Idiomas disponibles

La aplicación Citrix Workspace para iOS está adaptada para usarse en otros idiomas que no son el inglés. Para obtener una lista de los idiomas disponibles en la aplicación Citrix Workspace para iOS, consulte [Idiomas disponibles](#).

### Artículos de referencia

- [Resumen técnico: Citrix Workspace](#)
- [Global App Configuration Service](#)
- [Interfaz de usuario \(IU\) de Workspace](#)
- [Optimización de Microsoft Teams en entornos de Citrix Virtual Apps and Desktops](#)
- [Calendarios de publicación de versiones de la aplicación Citrix Workspace](#)
- [Documentación para desarrolladores](#)

### Novedades en los productos relacionados

- [Citrix Workspace](#)
- [Citrix DaaS](#)
- [StoreFront](#)
- [Secure Private Access](#)
- [Aplicación Citrix Workspace para Mac](#)

## Documentación antigua

Para ver las versiones de productos que han alcanzado el fin de su vida (EOL), consulte [Documentación antigua](#).

## Acerca de esta versión

July 1, 2024

Conozca las nuevas funciones, las mejoras, los problemas resueltos y los problemas conocidos.

### Nota:

¿Busca Technical Previews? Hemos seleccionado una lista para que pueda tenerlas en un solo lugar. Explore nuestra página [Funciones en Technical Preview](#) y comparta sus comentarios mediante los enlaces adjuntos al formulario de Podio.

## Novedades de la versión 24.5.0

### Función de autenticación mediante FIDO2 al conectarse a almacenes de la nube

A partir de la versión 24.5.0, los usuarios pueden autenticarse en la aplicación Citrix Workspace mediante la autenticación sin contraseña basada en FIDO2 al conectarse a almacenes de la nube. FIDO2 ofrece un método de autenticación integrado que permite a los empleados de la empresa acceder a aplicaciones y escritorios dentro de sesiones virtuales sin necesidad de introducir un nombre de usuario o una contraseña. Esta función admite tanto itinerancia (solo USB) como autenticadores de plataforma (código PIN, Touch ID y Face ID). Esta función está habilitada de manera predeterminada. Para obtener más información, consulte [Función de autenticación mediante FIDO2 al conectarse a almacenes de la nube](#).

### Nota:

De forma predeterminada, la autenticación FIDO2 es compatible con las fichas personalizadas de Chrome. Si le interesa usar la autenticación FIDO2 con WebView, registre su interés utilizando este [formulario de Podio](#).

### Función disponible para escáner de documentos

A partir de la versión 24.5.0, la aplicación Citrix Workspace para iOS admite la función de escáner de documentos. Con esta función, ahora puede escanear y guardar varios documentos, todo ello dentro

de la sesión de escritorio. Esta función está habilitada de manera predeterminada. Para obtener más información, consulte [Función disponible para escáner de documentos](#).

**Anuncio de retirada del protocolo DTLS 1.0** Citrix tiene previsto retirar la compatibilidad con el protocolo DTLS 1.0. en versiones futuras. El protocolo alternativo es DTLS 1.2. Para obtener más información, consulte [Elementos retirados](#).

### Technical Preview

- Función disponible para inicio de sesión único para máquinas virtuales unidas a Microsoft Entra ID
- Función disponible para aplicar autenticación biométrica para acceder a la aplicación Citrix Workspace

Para obtener una lista completa de las funciones en Technical Preview, consulte la página [Funciones en Technical Preview](#).

### Problemas solucionados en la versión 24.5.0

- Es posible que observe que, al usar el escáner de códigos de barras en la sesión virtual, el texto no se puede escanear correctamente. [HDX-63675]

### Problemas conocidos en la versión 24.5.0

Es posible que note que el panel táctil del teclado mágico no funciona correctamente en la sesión virtual en un dispositivo iPad pro M4. Como solución temporal, puede utilizar un mouse externo (ya sea Bluetooth o con cable y un conector USB tipo C) para navegar por la pantalla de la sesión virtual. [HDX-66083]

### Versiones anteriores

En esta sección se proporciona información sobre las nuevas funciones y los problemas resueltos en las versiones anteriores que seguimos desarrollando. Para obtener más información sobre el ciclo de vida de estas versiones, consulte [Lifecycle Milestones for Citrix Workspace app and Citrix Receiver](#).

## 24.4.0

### Novedades

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

**Anuncio de retirada de los protocolos TLS 1.0 y TLS 1.1** Citrix tiene previsto retirar la compatibilidad con los protocolos TLS 1.0 y TLS 1.1 en versiones futuras. Los protocolos alternativos son TLS 1.2 o TLS 1.3. Para obtener más información, consulte [Elementos retirados](#).

### Problemas resueltos

- Al abrir la cámara del dispositivo desde la sesión de la aplicación virtual, es posible que la aplicación Citrix Workspace para iOS se cierre inesperadamente. [CVADHELP-24825]

### Problemas conocidos

No hay nuevos problemas conocidos.

## 24.3.5

### Novedades

**Compatibilidad con el lector de la utilidad para tarjetas inteligentes twocanoes** A partir de la versión 24.3.5, la aplicación Citrix Workspace para iOS admite los lectores de la utilidad para tarjetas inteligentes twocanoes. Para obtener más información acerca de los lectores de tarjetas inteligentes compatibles y los detalles de configuración, consulte [Tarjetas inteligentes](#).

#### Nota:

El lector USB-C de la utilidad para tarjetas inteligentes twocanoes es compatible tanto para el inicio de sesión virtual como para el inicio de sesión con la aplicación Citrix Workspace. Sin embargo, el lector Bluetooth de la utilidad para tarjetas inteligentes twocanoes solo es compatible con el inicio de sesión en la aplicación Citrix Workspace, y no con el inicio de sesión virtual.

**Función para configurar el nombre del dispositivo a través de UEM** A partir de la versión 24.3.5, la aplicación Citrix Workspace para iOS permite a los administradores asignar e identificar nombres de dispositivos basados en grupos de usuarios a través de Unified Endpoint Management (UEM). Para obtener más información, consulte [Función para configurar el nombre del dispositivo a través de UEM](#).

### Technical Preview

- Función para configurar los parámetros de la aplicación Citrix Workspace a través de UEM

Para obtener más información sobre esta Technical Preview, consulte [Funciones en la Technical Preview](#).

### **Problemas resueltos**

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

### **Problemas conocidos**

No hay nuevos problemas conocidos.

## **24.3.0**

### **Novedades**

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

### **Technical Preview**

- Función disponible para audio adaptativo

Para obtener más información sobre esta Technical Preview, consulte [Funciones en la Technical Preview](#).

### **Problemas resueltos**

Tras actualizar la aplicación Citrix Workspace para iOS a la versión 24.1.0, es posible que las aplicaciones basadas en el software Oracle Java Web Start no puedan introducir el teclado mediante el teclado virtual de la sesión. [CVADHELP-24645]

### **Problemas conocidos**

No hay nuevos problemas conocidos.

## **24.2.0**

### **Novedades**

**Compatibilidad con la eliminación de varios almacenes a la vez** A partir de la versión 24.2.0, la aplicación Citrix Workspace para iOS permite seleccionar varios almacenes y eliminarlos. Esta función mejora la experiencia del usuario al trabajar con varios almacenes. Esta función está habilitada de manera predeterminada. Para obtener más información, consulte [Compatibilidad con la eliminación de varios almacenes a la vez](#).

**Función que permite al administrador restringir a los usuarios cambiar el nombre del almacén**  
Anteriormente, los usuarios podían cambiar el nombre del almacén con la opción **Modificar cuenta**.

A partir de la versión 24.2.0, la aplicación Citrix Workspace para iOS ofrece a los administradores la opción de impedir a los usuarios cambiar el nombre del almacén. Con esta función, los administradores pueden identificar y mantener fácilmente la coherencia de los nombres de los almacenes. Para obtener más información, consulte [Función que permite al administrador restringir a los usuarios cambiar el nombre del almacén](#).

**Rellenar automáticamente el nombre del almacén** A partir de la versión 24.2.0, la aplicación Citrix Workspace para iOS permite al administrador actualizar los nombres de los almacenes y envía automáticamente los nombres de los almacenes actualizados a los usuarios. Esta función mejora la experiencia del usuario al eliminar la necesidad de intervenir manualmente cuando se actualiza el nombre del almacén. Para obtener más información, consulte [Rellenar automáticamente el nombre del almacén](#).

**Nota:**

Esta función solo tiene efecto si el administrador ha inhabilitado a los usuarios para cambiar el nombre del almacén.

**Technical Preview**

- Compatibilidad con Accesibilidad y VoiceOver

Para obtener más información sobre esta Technical Preview, consulte [Funciones en la Technical Preview](#).

**Problemas resueltos**

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

**Problemas conocidos**

No hay nuevos problemas conocidos.



## 24.1.0

### Novedades

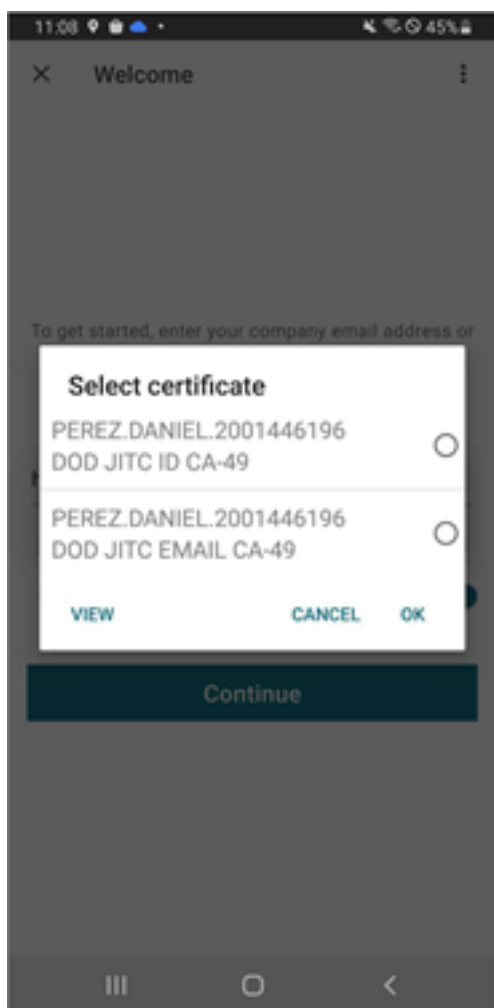
**Actualización de seguridad** Esta versión contiene actualizaciones de seguridad críticas y correcciones para problemas de seguridad.

**Función para configurar el almacenamiento de tokens de autenticación en la implementación local** La aplicación Citrix Workspace para iOS ofrece ahora una opción que permite configurar el almacenamiento de los tokens de autenticación en el disco local para los almacenes locales. Con esta función, puede inhabilitar el almacenamiento del token de autenticación para mejorar la seguridad. Tras la inhabilitación, cuando se reinicie el sistema o la sesión, tendrá que autenticarse de nuevo para acceder a la sesión. Para obtener más información, consulte [Función para configurar el almacenamiento de tokens de autenticación en la implementación local](#).

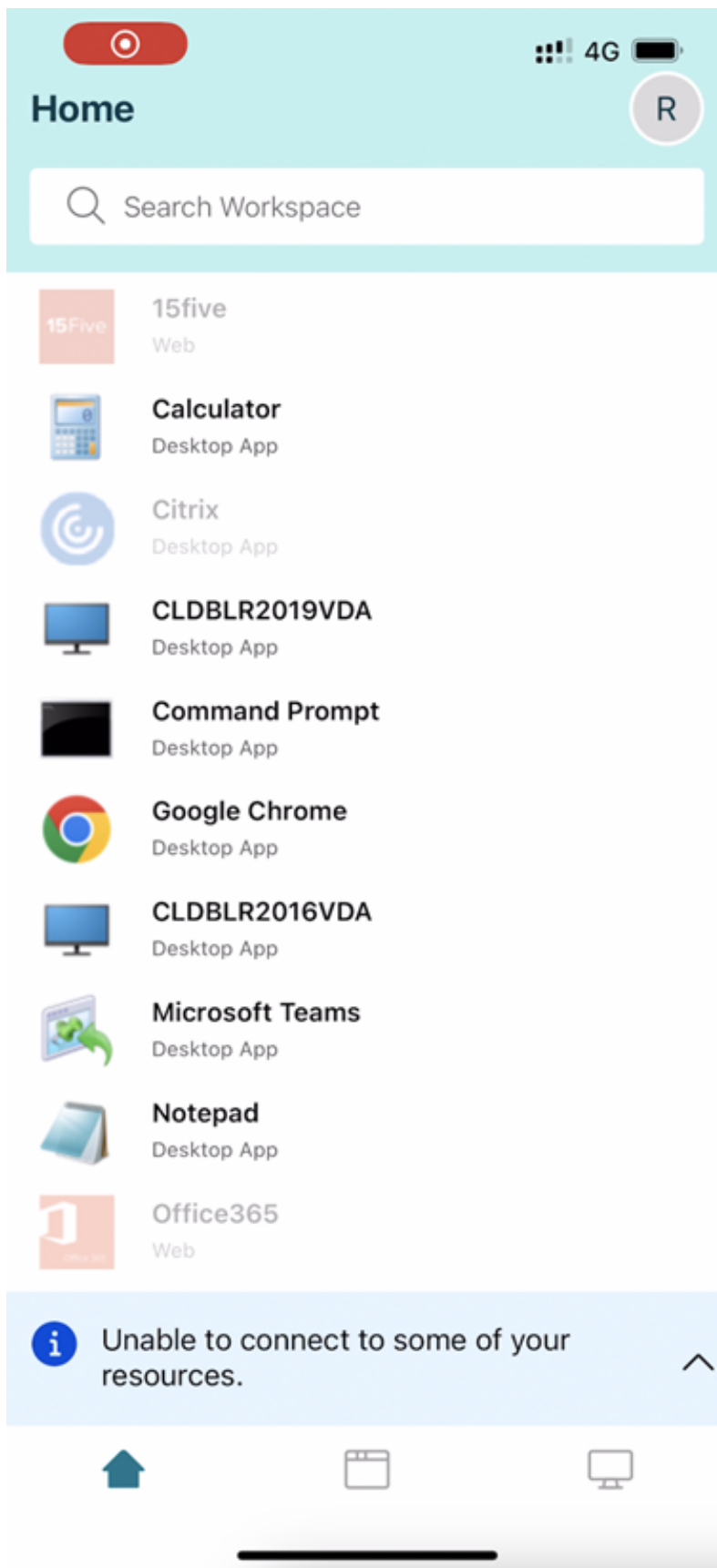
**Compatibilidad con varios almacenes de la nube** A partir de la versión 24.1.0, puede agregar varias cuentas de almacenamiento en la nube a la aplicación Citrix Workspace para iOS y iPadOS. Ahora, es fácil para los usuarios finales agregar almacenes y cambiar entre ellos. Esta función mejora la experiencia del usuario al acceder a varios almacenes. Para obtener más información, consulte [Compatibilidad con varios almacenes de la nube](#).

**Compatibilidad con varios certificados en la autenticación con tarjeta inteligente** Anteriormente, la aplicación Citrix Workspace para iOS mostraba el certificado disponible en la primera ranura de la tarjeta inteligente conectada.

A partir de la versión 24.1.0, la aplicación Citrix Workspace para iOS muestra todos los certificados disponibles en la tarjeta inteligente y le permite seleccionar el certificado necesario al autenticarse con tarjeta inteligente. Para obtener más información, consulte [Compatibilidad con varios certificados en la autenticación con tarjeta inteligente](#).



**Se ha mejorado la interfaz de usuario para el modo sin conexión de continuidad del servicio** A partir de la versión 24.1.0, la interfaz de usuario de la aplicación Citrix Workspace para iOS se ha mejorado para hacerla más informativa y moderna, así como para ofrecer una mejor experiencia durante las interrupciones del servicio. La función de búsqueda aproximada también se incluye para el modo sin conexión. Con esta función, puede encontrar resultados de aplicaciones o escritorios con texto parecido y términos de búsqueda mal escritos. Para obtener más información sobre la función de continuidad del servicio, consulte [Continuidad del servicio](#).

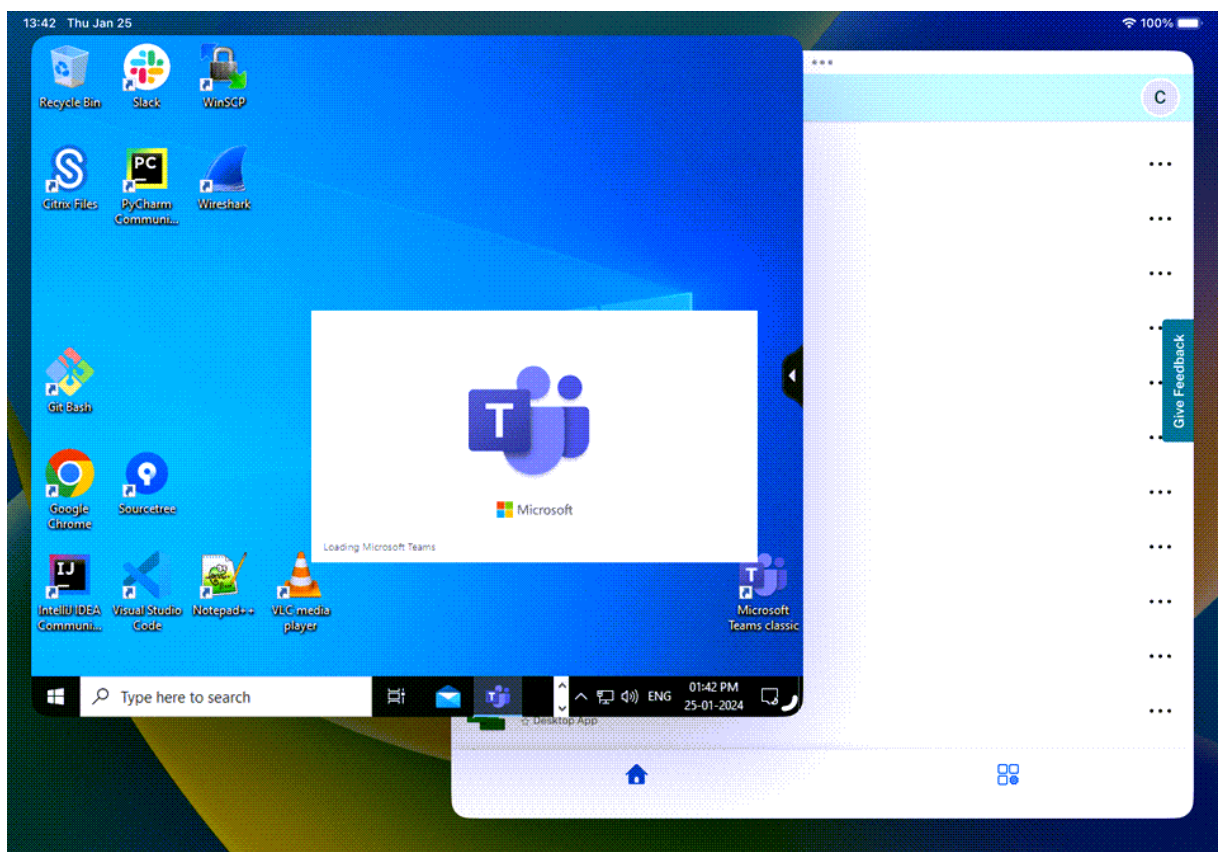


**Compatibilidad con ventanas de sesión independientes de la aplicación Citrix Workspace** A partir de la versión 24.1.0, la aplicación Citrix Workspace para iOS presenta una ventana de sesión independiente que hace que la multitarea sea más eficiente y fácil de usar. Con esta función, puede disfrutar de una experiencia similar a la de un escritorio. Cuando la función Ventana de sesión independiente está habilitada, puede simplemente puede arrastrar y colocar las sesiones en los monitores externos conectados. De esta forma, el monitor principal del iPad se puede usar en modo multitarea con otras aplicaciones.

**Nota:**

Esta función solo es compatible en los dispositivos que admiten la función Organizador visual. Todos los dispositivos iPhone y algunos dispositivos iPad no admiten esta función. Para obtener más información sobre la función Organizador visual, consulte [Activar o desactivar el organizador visual en el iPad](#) en la documentación de asistencia de Apple.

Para obtener más información, consulte [Compatibilidad con ventanas de sesión independientes de la aplicación Citrix Workspace](#).



**Compatibilidad con el modo de entrada de texto Scancode** A partir de la versión 24.1.0, puede seleccionar **Scancode** como modo de entrada del teclado mientras usa un teclado físico externo. Esta

función resulta útil cuando usa dispositivos iOS con un teclado estándar externo para PC con Windows. Con **Scancode**, puede usar la distribución del teclado del VDA en lugar del teclado virtual de iOS. De esta forma, puede seguir completamente el estilo de entrada del teclado externo de Windows en lugar de iOS. Eso resulta muy útil cuando se escribe en idiomas de Asia oriental, ya que mejora significativamente la experiencia general del usuario. Es posible que el usuario final use la distribución del teclado del servidor en lugar de usar la del cliente. Para obtener más información, consulte [Compatibilidad con el modo de entrada de texto Scancode](#).

**Mejora de la compatibilidad con accesos directos de teclados externos** La aplicación Citrix Workspace para iOS ahora le permite usar más accesos directos de teclados externos en una sesión de escritorio o aplicación remotos. Las siguientes son mejoras importantes realizadas en los accesos directos de teclados externos:

- Compatibilidad con teclas específicas del teclado Windows, como [Insert](#), [Delete](#) y el teclado numérico.
- Si mantiene presionada una tecla y no la suelta, la aplicación o el escritorio remoto responden correctamente.
- Compatibilidad con accesos directos de más de tres teclas.

Además, ahora puede configurar la tecla específica de [Alt](#) mediante las siguientes opciones de **Parámetros > Opciones de teclado > Asignar tecla específica para Alt**:

- [Option or Alt \(left\)](#): Envía [Alt](#) mediante [Option \(left\)](#) or [Alt \(left\)](#).
- [Command or Windows \(left\)](#): Envía [Alt](#) mediante las teclas [Command \(left\)](#) or [Windows \(left\)](#).
- [Option or Alt \(left and right\)](#): Envía [Alt](#) mediante la tecla [Option or Alt \(left and right\)](#).

La opción **Asignar tecla específica para Alt** ayuda a evitar conflictos entre la tecla [Option](#) de macOS y la tecla [Alt](#) de Windows.

Para obtener más información, consulte [Mejora de la compatibilidad con accesos directos de teclados externos](#).

**Rendimiento gráfico mejorado** A partir de la versión 24.1.0, la aplicación Citrix Workspace para iOS admite la codificación o decodificación de vídeo H.264 acelerada por hardware. Ahora, el motor multimedia de Citrix HDX usa el marco Video Toolbox de Apple para la codificación y la decodificación. Este marco comprime y descomprime vídeo más rápido y en tiempo real. Esta mejora reduce la carga de la CPU durante el uso multimedia. Para obtener más información, consulte [Rendimiento gráfico mejorado](#).

## Problemas resueltos

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

## Problemas conocidos

- Tras actualizar la aplicación Citrix Workspace para iOS a la versión 24.1.0, es posible que las aplicaciones basadas en el software Oracle Java Web Start no puedan introducir el teclado mediante el teclado virtual de la sesión. [CVADHELP-24645]

### 23.12.1

## Novedades

**Compatibilidad con YubiKey para la autenticación con tarjeta inteligente** Ahora puede realizar la autenticación con tarjeta inteligente con YubiKey. Esta función proporciona una experiencia de autenticación de un solo dispositivo para la aplicación Citrix Workspace, las sesiones virtuales y las aplicaciones publicadas en la sesión del VDA. Elimina la necesidad de conectar lectores de tarjetas inteligentes u otros autenticadores externos. Simplifica la experiencia del usuario final, ya que YubiKey es compatible con una amplia variedad de protocolos, como OTP, FIDO, etc.

Para iniciar sesión en la aplicación Citrix Workspace, inserte la YubiKey en el iPhone o iPad, active la opción de tarjeta inteligente y proporcione la URL de almacén.

#### Nota:

La aplicación Citrix Workspace para iOS solo admite la serie YubiKey 5. Para obtener más información sobre YubiKey, consulte la [serie YubiKey 5](#).

**Soporte para lectores genéricos basados en el tipo C** La aplicación Citrix Workspace para iOS ahora admite lectores compatibles con el CCID de tipo C para la autenticación con tarjetas inteligentes. Anteriormente, solo eran compatibles los lectores basados en puertos Lightning. La inclusión de lectores de tarjetas inteligentes tipo C en la aplicación Citrix Workspace ofrece una doble ventaja: los usuarios pueden autenticarse a través de la aplicación Citrix Workspace y utilizar la tarjeta inteligente sin problemas en sus sesiones de escritorio virtual.

**Configurar el nombre del dispositivo a través de UEM** Con esta versión, un nuevo parámetro denominado `deviceName` ya está disponible para la configuración a través de Unified Endpoint Management (UEM). Este atributo ayuda a los administradores a asignar e identificar los nombres de los dispositivos según los grupos de usuarios.

Clave de configuración	Tipo de valor	Valor de configuración
deviceName	Cadena	nombre_del_dispositivo

**No disponible para la versión 14 de iOS** La aplicación Citrix Workspace para iOS no es compatible con la versión 14 de iOS o anteriores a partir de la 23.12.0. Puede actualizar a la versión más reciente de iOS desde la App Store. Para obtener más información, consulte la [Tabla de elementos retirados](#).

### Technical Preview

- Compatibilidad con cámaras web externas

Para obtener más información sobre esta Technical Preview, consulte [Funciones en la Technical Preview](#).

### Problemas resueltos

- El inicio de la sesión de escritorio falla cuando el idioma de la aplicación Citrix Workspace se establece en italiano.

## 23.12.0

### Novedades

**Compatibilidad con YubiKey para la autenticación con tarjeta inteligente** Ahora puede realizar la autenticación con tarjeta inteligente con YubiKey. Esta función proporciona una experiencia de autenticación de un solo dispositivo para la aplicación Citrix Workspace, las sesiones virtuales y las aplicaciones publicadas en la sesión del VDA. Elimina la necesidad de conectar lectores de tarjetas inteligentes u otros autenticadores externos. Simplifica la experiencia del usuario final, ya que YubiKey es compatible con una amplia variedad de protocolos, como OTP, FIDO, etc.

Para iniciar sesión en la aplicación Citrix Workspace, inserte la YubiKey en el iPhone o iPad, active la opción de tarjeta inteligente y proporcione la URL de almacén.

#### Nota:

La aplicación Citrix Workspace para iOS solo admite la serie YubiKey 5. Para obtener más información sobre YubiKey, consulte la [serie YubiKey 5](#).

**Soporte para lectores genéricos basados en el tipo C** La aplicación Citrix Workspace para iOS ahora admite lectores compatibles con el CCID de tipo C para la autenticación con tarjetas inteligentes. Anteriormente, solo eran compatibles los lectores basados en puertos Lightning. La inclusión de lectores de tarjetas inteligentes tipo C en la aplicación Citrix Workspace ofrece una doble ventaja: los usuarios pueden autenticarse a través de la aplicación Citrix Workspace y utilizar la tarjeta inteligente sin problemas en sus sesiones de escritorio virtual.

**Configurar el nombre del dispositivo a través de UEM** Con esta versión, un nuevo parámetro denominado `deviceName` ya está disponible para la configuración a través de Unified Endpoint Management (UEM). Este atributo ayuda a los administradores a asignar e identificar los nombres de los dispositivos según los grupos de usuarios.

---

Clave de configuración	Tipo de valor	Valor de configuración
<code>deviceName</code>	Cadena	<code>nombre_del_dispositivo</code>

---

**No disponible para la versión 14 de iOS** La aplicación Citrix Workspace para iOS no es compatible con la versión 14 de iOS o anteriores a partir de la 23.12.0. Puede actualizar a la versión más reciente de iOS desde la App Store. Para obtener más información, consulte la [Tabla de elementos retirados](#).

### Technical Preview

- Compatibilidad con cámaras web externas

Para obtener más información sobre esta Technical Preview, consulte [Funciones en la Technical Preview](#).

### Problemas resueltos

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

## 23.12.0

### Novedades

**Compatibilidad con YubiKey para la autenticación con tarjeta inteligente** Ahora puede realizar la autenticación con tarjeta inteligente con YubiKey. Esto proporciona una experiencia de autenticación de un solo dispositivo para aplicaciones web y SaaS y sesiones virtuales y elimina la necesidad



de conectar lectores de tarjetas inteligentes u otros autenticadores externos. Simplifica la experiencia del usuario final, ya que YubiKey es compatible con una amplia variedad de protocolos, como OTP, FIDO, etc.

Para iniciar sesión en la aplicación Citrix Workspace, inserte la YubiKey en el iPhone o iPad, active la opción de tarjeta inteligente y proporcione la URL de almacén.

**Nota:**

La aplicación Citrix Workspace para iOS solo admite la serie YubiKey 5. Para obtener más información sobre YubiKey, consulte la [serie YubiKey 5](#).

**Soporte para lectores genéricos basados en el tipo C** La aplicación Citrix Workspace para iOS ahora admite lectores compatibles con el CCID de tipo C para la autenticación con tarjetas inteligentes. Anteriormente, solo eran compatibles los lectores basados en puertos Lightning. La inclusión de lectores de tarjetas inteligentes tipo C en la aplicación Citrix Workspace ofrece una doble ventaja: los usuarios pueden autenticarse a través de la aplicación Citrix Workspace y utilizar la tarjeta inteligente sin problemas en sus sesiones de escritorio virtual.

**Configurar el nombre del dispositivo a través de UEM** Con esta versión, un nuevo parámetro denominado `deviceName` ya está disponible para la configuración a través de Unified Endpoint Management (UEM). Este atributo ayuda a los administradores a asignar e identificar los nombres de los dispositivos según los grupos de usuarios.

---

Clave de configuración	Tipo de valor	Valor de configuración
<code>deviceName</code>	Cadena	<code>nombre_del_dispositivo</code>

---

**No disponible para la versión 14 de iOS** La aplicación Citrix Workspace para iOS no es compatible con la versión 14 de iOS o anteriores a partir de la 23.12.0. Puede actualizar a la versión más reciente de iOS desde la App Store. Para obtener más información, consulte la [Tabla de elementos retirados](#).

### Technical Preview

- Compatibilidad con cámaras web externas

Para obtener más información sobre esta Technical Preview, consulte [Funciones en la Technical Preview](#).

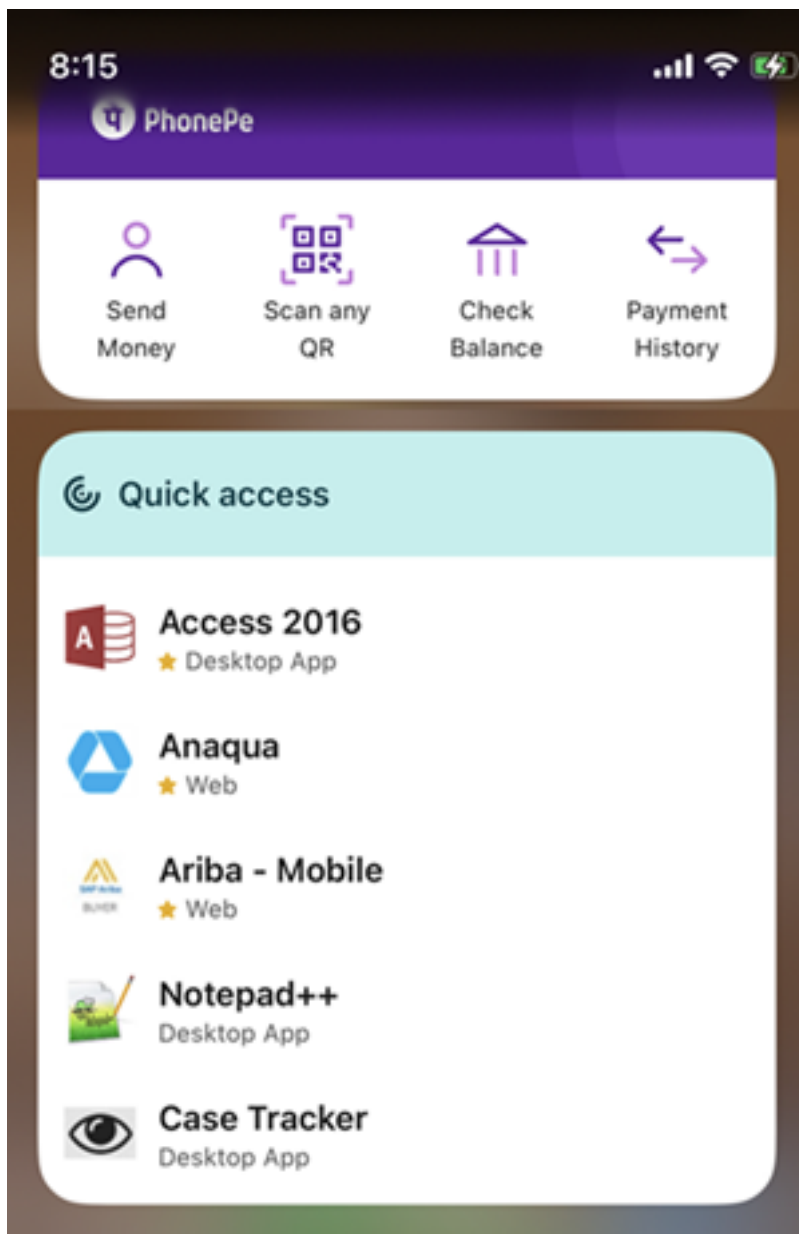
## **Problemas resueltos**

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

### **23.11.0**

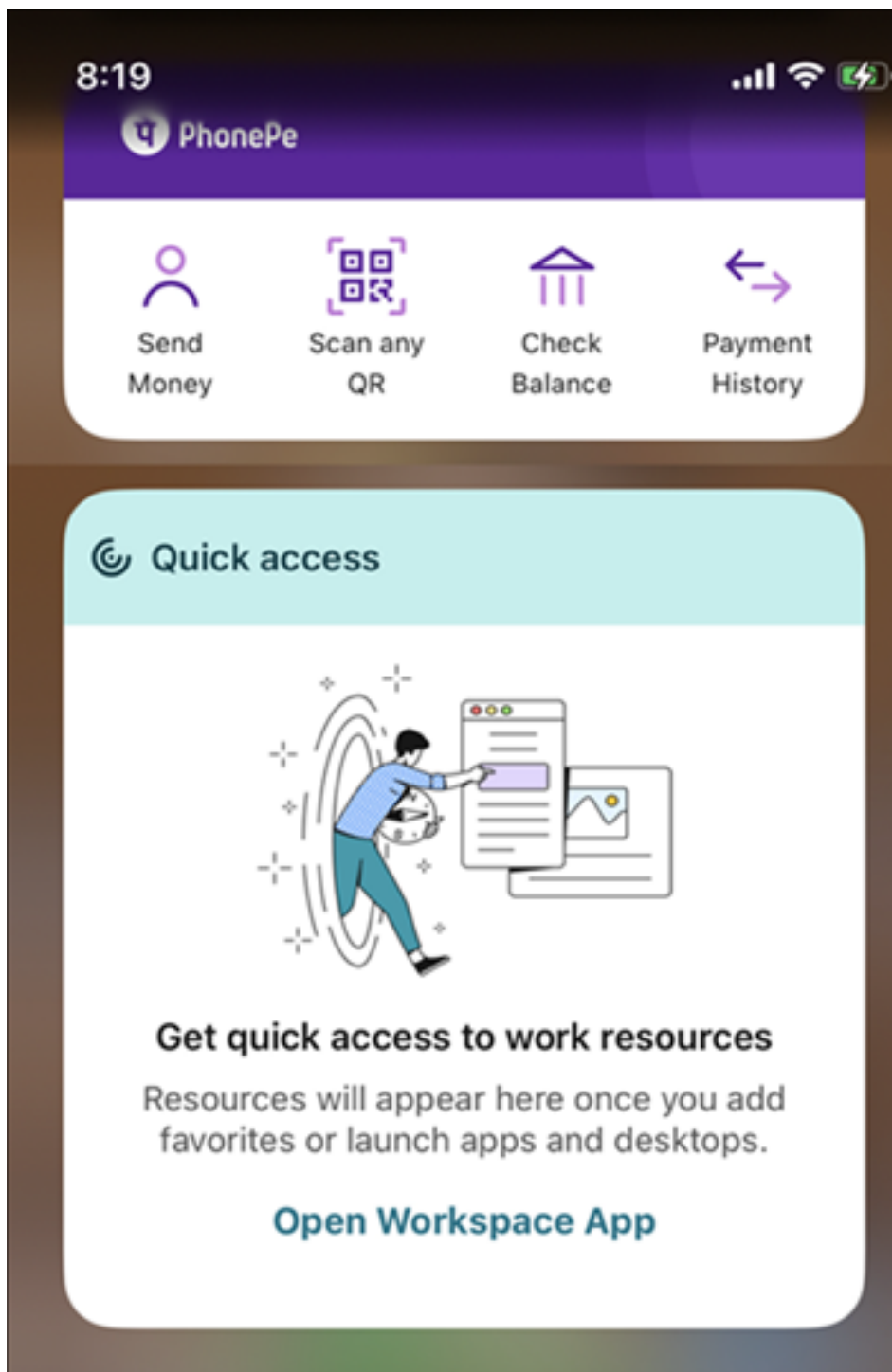
#### **Ver aplicaciones y escritorios como widgets**

Los usuarios finales ahora pueden iniciar sus aplicaciones y escritorios virtuales directamente desde sus dispositivos iPhone y iPad. No necesitan abrir la aplicación Citrix Workspace para iniciar una sesión de escritorio o aplicación. Un usuario puede tener un máximo de 5 Virtual Apps and Desktops como widgets.



Los widgets se crean automáticamente conforme a los siguientes criterios:

- 3 aplicaciones o escritorios favoritos y 2 abiertos recientemente se muestran como widgets.
- Si no hay aplicaciones o escritorios favoritos, se muestran como widgets hasta cinco aplicaciones y escritorios abiertos recientemente
- Si no hay aplicaciones o escritorios abiertos recientemente, se muestran hasta cinco aplicaciones o escritorios favoritos como widgets
- Si aún no se ha agregado ninguna aplicación o escritorio como favorito y no se ha abierto ninguna aplicación o escritorio recientemente, se pide a los usuarios que abran la aplicación Citrix Workspace para iOS. A continuación, pueden marcar determinadas aplicaciones o escritorios como favoritos.



### Problemas resueltos

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

### 23.10.1

#### **Novedades**

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

#### **Problemas resueltos**

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

### 23.10.0

#### **Novedades**

**Anuncio de fin de compatibilidad con la versión 14 de iOS** La aplicación Citrix Workspace no admitirá la versión 14 de iOS ni versiones anteriores a partir de versión 23.12.0. Puede actualizar a la versión más reciente de iOS desde la App Store. Para obtener más información, consulte la tabla de [elementos retirados](#).

#### **Problemas resueltos**

En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

### 23.9.0

#### **Novedades**

**Compatibilidad con Transport Layer Security 1.3** Ahora, la aplicación Citrix Workspace para iOS es compatible con Transport Layer Security (TLS) 1.3, que mejora el rendimiento y la eficiencia. TLS 1.3 proporciona una gran seguridad con sus robustos conjuntos de cifrado y sus claves de sesión de un solo uso.

Los usuarios finales pueden habilitarlo en la aplicación Citrix Workspace para iOS de esta manera:

1. Vaya a **Parámetros avanzados > Versiones de TLS**.
2. Seleccione la **Versión de TLS 1.3**.

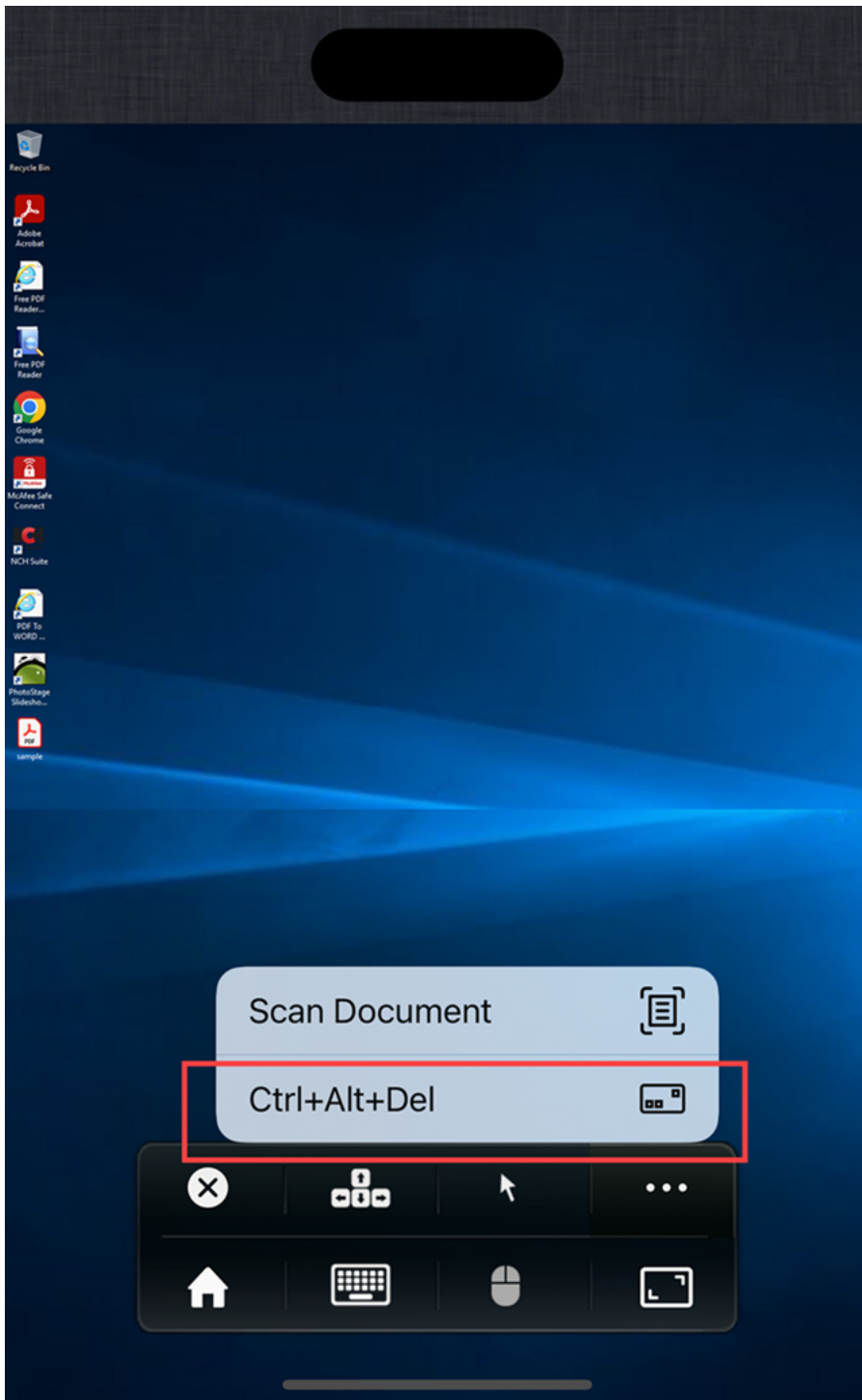
**Función para impresoras compatibles con AirPrint** Ahora, con las impresoras compatibles con la tecnología AirPrint, los usuarios finales pueden imprimir documentos desde sus sesiones activas en dispositivos iOS. Así, no hace falta tener las impresoras conectadas por cable o red. Las impresoras compatibles con AirPrint aparecen junto con las demás impresoras disponibles cuando los usuarios inician un comando de impresión.

Para imprimir con una impresora compatible con AirPrint, los usuarios deben asegurarse de lo siguiente.

- La impresora requerida debe ser compatible con AirPrint y estar habilitada para AirPrint.
- El dispositivo del usuario debe estar conectado a la misma red Wi-Fi que la impresora compatible con AirPrint.

Esta funcionalidad está disponible para las plataformas iOS tanto en entornos locales como de la nube.

**Incorporación del acceso directo Ctrl+Alt+Supr a la barra de herramientas de la sesión** Ahora, la barra de herramientas de la sesión tiene una opción para realizar la función **Ctrl+Alt+Supr** con solo tocar un botón. Esta opción facilita a los usuarios cerrar sesión, cambiar de usuario, bloquear el sistema o acceder al Administrador de tareas.



**Autenticación basada en FIDO2** La aplicación Citrix Workspace para iOS ahora admite la autenticación sin contraseña dentro de una sesión de Citrix Virtual Apps and Desktops mediante métodos de autenticación basados en FIDO2. Esto permite a los usuarios iniciar sesión en un sitio web compatible con WebAuthn en exploradores como Google Chrome o Microsoft Edge mediante claves de seguridad

Yubico compatibles con FIDO2. El simple hecho de abrir un sitio web compatible con WebAuthn desencadena la autenticación sin contraseña.

Solo se admiten dispositivos con puertos Lightning (no se admiten dispositivos con puertos USB-C o USB 4). No se admite el inicio de sesión en la aplicación Citrix Workspace o en la sesión de escritorio mediante autenticación sin contraseña.

Para obtener más información sobre los requisitos previos de esta función, consulte [Autorización local y autenticación virtual mediante FIDO2](#) en la documentación de Citrix Virtual Apps and Desktops.

### Technical Preview

- Agregar varios almacenes mediante Unified Endpoint Management (UEM)
- Eliminar varios almacenes mediante Unified Endpoint Management (UEM)

Para obtener la lista completa de las funciones en Technical Preview, consulte la página [Funciones en Technical Preview](#).

### Problemas resueltos

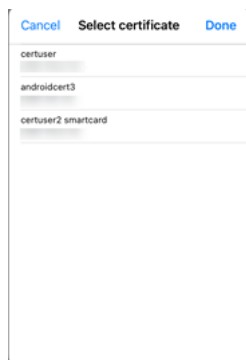
En esta versión, se trató una serie de áreas para mejorar la estabilidad y el rendimiento general.

## 23.7.5

### Novedades

#### Ver todos los certificados disponibles en la tarjeta inteligente

Ahora, la aplicación Citrix Workspace para iOS muestra varios certificados disponibles en la tarjeta inteligente y le permite seleccionar el certificado para la autenticación basada en tarjetas inteligentes. El certificado necesario se puede seleccionar en la página **Seleccionar certificado** una vez que se haya habilitado el botón de tarjetas inteligentes.





### **Acceso a almacenes web habilitados para Global App Configuration Service**

Ahora, los administradores pueden configurar almacenes web (interfaces web) para la detección de almacenes por correo electrónico. En función de la dirección de correo electrónico que introdujeron los usuarios finales al agregar un almacén (en la pantalla de bienvenida), Global App Configuration Service ayuda a identificar la URL de la web personalizada (interfaz web) definida por el administrador. A continuación, se dirige automáticamente al usuario final al almacén web configurado por el administrador.

Para obtener más información sobre la configuración de las URL de almacenes web para los usuarios finales, consulte [Allowed custom web portal](#).

### **Anuncio de retirada de PNAgent**

Anunciamos la retirada del almacén de PNA para la aplicación Citrix Workspace para iOS en la versión 23.7.5. Citrix no ofrecerá correcciones de errores ni parches de seguridad para la función de almacenamiento de PNA posteriores a la versión 23.7.5.

### **Problemas resueltos**

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.

### **23.6.5**

#### **Novedades**

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.

#### **Problemas resueltos**

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.

## 23.6.0

### Novedades

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.

### Problemas resueltos

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.

## 23.5.0

### Novedades

**Mejoras en el teclado extendido** A partir de la versión 23.5.0, se ha mejorado la funcionalidad de teclado extendido para ofrecer una mejor experiencia de usuario. Las mejoras son las siguientes:

- Anclaje o desanclaje de la interfaz de usuario de la barra de herramientas extendida.
- Rotación de la barra de herramientas extendida en sincronía con la rotación de la pantalla.
- Compatibilidad con la tecla con el logotipo de Windows y los accesos directos que son combinación de 3 teclas.
- Mejora de la experiencia cuando se utilizan varios monitores.
- Apertura y contracción automáticas de la interfaz de usuario de la barra de herramientas extendida.
- Mejora de la experiencia en el modo del organizador visual (en iPad con chip M1).

**Problemas resueltos en la versión 23.5.0** En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.

## 23.4.5

### Novedades

**Compatibilidad con canales de Global App Configuration Service** Ahora, a partir de la versión 23.4.5, los administradores pueden usar Global App Configuration Service para definir parámetros y probarlos antes de implementar la configuración para todos los usuarios finales. Este proceso garantiza una prueba minuciosa de las funciones y funcionalidades antes de cambiar a un entorno de producción.

**Nota:**

- La aplicación Citrix Workspace para iOS admite las configuraciones **Predeterminado** y **Canal de prueba**. De forma predeterminada, todos los usuarios están en el canal **Predeterminado**.

Para obtener más información, consulte la documentación de [Global App Configuration Service](#).

Para obtener más información sobre cómo configurar, consulte [Compatibilidad con canales de Global App Configuration Service](#).

**Función para configurar almacenes mediante soluciones de MDM** Ahora, la aplicación Citrix Workspace para iOS permite la configuración remota de la URL del almacén de Workspace mediante soluciones de administración de dispositivos móviles (MDM). Para obtener más información, consulte [Configurar la aplicación Workspace mediante soluciones de MDM](#).

**Mejoras en las soluciones de MDM** La aplicación Citrix Workspace para iOS admite un par de configuraciones más mediante pares de clave-valor basados en AppConfig para configurar la aplicación Citrix Workspace. Anteriormente, los administradores podían configurar las URL de los almacenes. Ahora, los administradores pueden restringir a los usuarios finales la posibilidad de modificar las URL de los almacenes y controlar la apariencia de la aplicación.

Configuration key	Value type	Configuration value
url	String	myworkprod0.cloud.com
restrict_user_store_modification	Boolean	true
storeType	Integer	1

Estos son los detalles:

---

Clave de configuración	Tipo de valor	Valor de configuración
url	String	La URL del almacén. Por ejemplo, <code>prodcwa.cloud.com</code>

Clave de configuración	Tipo de valor	Valor de configuración
<code>storeType</code>	<code>Integer</code>	<ul style="list-style-type: none"><li>• (predeterminado) Si se establece en 1, los usuarios pueden ver la carga nativa o predeterminada del almacén. - Si se establece en 2, los usuarios pueden ver el almacén dentro de una interfaz web.</li></ul>
<code>restrict_user_store_modification</code>	<code>Boolean</code>	<ul style="list-style-type: none"><li>• Si se establece en <b>true</b>, los usuarios no pueden modificar el almacén (agregar/eliminar/modificar). - Si se establece en <b>false</b>, los usuarios pueden modificar el almacén. <b>Nota:</b> Si el indicador se establece en <b>true</b>, se eliminarán todos los almacenes existentes antes de agregar uno nuevo configurado por MDM.</li></ul>

---

### Technical Preview

- Compatibilidad con autenticación basada en FIDO2

Para obtener una lista completa de las funciones en Technical Preview, consulte la página [Funciones en Technical Preview](#).

### Problemas resueltos en la versión 23.4.5

- Cuando se activa el modo de desplazamiento natural y se mueven los dedos de arriba a abajo en el iPad, la página se mueve hacia abajo. Se observa el mismo comportamiento incluso al desactivar el desplazamiento natural. Además, este comportamiento también se observa con Magic Mouse. [HDX-49267]

- En el modo Ampliar, cuando se utiliza una resolución “Ajuste automático - Media” o “Ajuste automático - Alta”, la resolución de la pantalla se escala automáticamente y la pantalla se trunca. Este problema ocurre cuando la aplicación Citrix Workspace pasa del segundo plano al primer plano. [CVADHELP-19169]

## 23.3.5

### Novedades

**Cadena de usuario-agente** De forma predeterminada, la cadena de usuario-agente utilizada durante algunas de las solicitudes de red iniciadas a través de WKWebView incluye ahora el identificador de la aplicación Citrix Workspace.

Por lo tanto, se ha cambiado de:

```
Mozilla/5.0 (iPhone; CPU iPhone OS 15_2 like Mac OS X) AppleWebKit  
/605.1.15 (KHTML, like Gecko) Mobile/15E148 AuthManager/3.2.4.0
```

A una de las siguientes opciones:

```
Mozilla/5.0 (iPhone; CPU iPhone OS 15_0 like Mac OS X) AppleWebKit  
/605.1.15 (KHTML, like Gecko) Mobile/15E148 CWA/23.3.0 iOS/15.0  
X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPhone  
(iPhone de ejemplo)
```

O bien,

```
Mozilla/5.0 (iPhone; CPU iPhone OS 15_0 like Mac OS X) AppleWebKit  
/605.1.15 (KHTML, like Gecko) Mobile/15E148 CWA/23.3.0 iOS/15.0  
X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPad  
(iPad de ejemplo)
```

### Technical Previews

- Escaneo rápido

Para obtener una lista completa de las funciones en Technical Preview, consulte la página [Funciones en Technical Preview](#).

### Problemas resueltos en la versión 23.3.5

Tras actualizar la aplicación Citrix Workspace para iOS a la versión 23.3.0, no podrá autenticarse en su almacén si este está configurado con la dirección completa del almacén a través de una solución de MDM.

## 23.3.0

### Novedades

#### **Función para configurar almacenes mediante soluciones de MDM [Technical Preview]**

**Nota:**

Esta función se encuentra en Tech Preview.

Ahora, la aplicación Citrix Workspace para iOS permite la configuración remota de la URL del almacén de Workspace mediante soluciones de administración de dispositivos móviles (MDM). Para obtener más información, consulte [Configurar la aplicación Workspace mediante soluciones de MDM](#).

**Reautenticación después de agotarse el tiempo de espera de la sesión** Ahora, con esta versión, se le pedirá autenticarse de nuevo en la aplicación Citrix Workspace si la sesión caducó desde su último inicio de sesión. Se le solicitará la autenticación de dos factores o un nombre de usuario y una contraseña cuando se conecte a la aplicación Citrix Workspace desde la web o desde un cliente nativo.

### Technical Preview

- Escáner de documentos
- Compatibilidad con PiP

Para obtener una lista completa de las funciones en Technical Preview, consulte la página [Funciones en Technical Preview](#).

### Problemas resueltos

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.

## 23.2.1

### Novedades

**Compatibilidad con cámara trasera** La aplicación Citrix Workspace para iOS ahora permite cambiar la posición de la cámara de frontal a trasera y viceversa dentro de una sesión HDX.

Al invocar la cámara en la sesión virtual, en la pantalla se muestra un botón flotante de cámara que permite cambiar la posición de la cámara. También puede mover el botón flotante libremente por la pantalla y colocarlo donde quiera.

Para cambiar la posición de la cámara entre las posiciones frontal y trasera en las sesiones virtuales, siga estos pasos:

1. Abra una aplicación cliente que captura vídeo.
2. Inicie la grabación del vídeo.
3. Toque el botón flotante de la cámara que se muestra en la pantalla para cambiar entre la cámara frontal y la trasera.

**Nota:**

Los parámetros de la aplicación cliente no afectan a la cámara durante una sesión HDX. Debe usar el botón flotante de la cámara que Citrix habilita para cambiar la posición de la cámara.

**Problemas conocidos:**

El botón flotante queda tapado parcial o totalmente cuando la función de proyección o la función de escaneo de documentos se habilitan.

**Función para rellenar automáticamente la URL del almacén** Al acceder a la aplicación Citrix Workspace para iOS con una nueva personalización de marca, puede elegir rellenar automáticamente la URL del almacén. Esta función reduce las intervenciones manuales y proporciona un acceso rápido a la aplicación. Para obtener más información sobre la personalización de aplicaciones, consulte [App Personalization](#).

**Función para cambiar de explorador web para la autenticación** En dispositivos iOS o iPad, los administradores ya pueden cambiar el explorador web que se utiliza para el proceso de autenticación del explorador web integrado al explorador web del sistema al configurar una directiva de autenticación avanzada en la implementación local de Citrix Gateway y StoreFront. Para obtener más información, consulte [Configurar la directiva de reescritura para el proceso de autenticación](#).

**Problemas resueltos**

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.

### 23.2.0

**Novedades**

**Compatibilidad con cámara trasera** La aplicación Citrix Workspace para iOS ahora permite cambiar la posición de la cámara de frontal a trasera y viceversa dentro de una sesión HDX.

Al invocar la cámara en la sesión virtual, en la pantalla se muestra un botón flotante de cámara que permite cambiar la posición de la cámara. También puede mover el botón flotante libremente por la pantalla y colocarlo donde quiera.

Para cambiar la posición de la cámara entre las posiciones frontal y trasera en las sesiones virtuales, siga estos pasos:

1. Abra una aplicación cliente que captura vídeo.
2. Inicie la grabación del vídeo.
3. Toque el botón flotante de la cámara que se muestra en la pantalla para cambiar entre la cámara frontal y la trasera.

**Nota:**

Los parámetros de la aplicación cliente no afectan a la cámara durante una sesión HDX. Debe usar el botón flotante de la cámara que Citrix habilita para cambiar la posición de la cámara.

**Problemas conocidos:**

El botón flotante queda tapado parcial o totalmente cuando la función de proyección o la función de escaneo de documentos se habilitan.

**Función para rellenar automáticamente la URL del almacén** Al acceder a la aplicación Citrix Workspace para iOS con una nueva personalización de marca, puede elegir rellenar automáticamente la URL del almacén. Esta función reduce las intervenciones manuales y proporciona un acceso rápido a la aplicación. Para obtener más información sobre la personalización de aplicaciones, consulte [App Personalization](#).

**Función para cambiar de explorador web para la autenticación** En dispositivos iOS o iPad, los administradores ya pueden cambiar el explorador web que se utiliza para el proceso de autenticación del explorador web integrado al explorador web del sistema al configurar una directiva de autenticación avanzada en la implementación local de Citrix Gateway y StoreFront. Para obtener más información, consulte [Configurar la directiva de reescritura para el proceso de autenticación](#).

**Problemas resueltos**

En esta versión se han resuelto una serie de problemas para mejorar la estabilidad y el rendimiento generales.



## Limitaciones

- Le recomendamos que utilice las teclas **Control + C** y **Control + V** del teclado en pantalla de su dispositivo para copiar y pegar contenido. Es posible que no funcionen las teclas **Comando + C** y **Comando + V** de un teclado externo. [HDX-32431]
- No se pueden iniciar aplicaciones si se toca el archivo ICA en el gestor de descargas al utilizar el explorador web Safari.  
Para garantizar que las aplicaciones se inicien correctamente desde Safari, compruebe que la versión más reciente de la aplicación Citrix Workspace o Citrix Receiver para iOS (pero no ambas) esté presente en el dispositivo. [RFIOS-5502]
- Tras migrar a Citrix Workspace desde StoreFront, la pantalla parpadea momentáneamente al tocar el botón **Siguiente** de la guía sobre Pendo.
- Al iniciar aplicaciones web y SaaS desde la aplicación Citrix Workspace, si la aplicación usa el IDP de Google y requiere que el usuario inicie sesión, la autenticación fallará y aparecerá el mensaje de error “Acceso denegado”. [RFIOS-11904]

## Elementos retirados

Para obtener información sobre los elementos retirados, consulte la página [Elementos retirados](#).

## Funciones en Technical Preview











July 1, 2024

Las funciones en versión Technical Preview están disponibles para uso en entornos de producción limitados o en entornos que no son de producción, y para dar a los clientes la oportunidad de compartir comentarios. Citrix no acepta casos de asistencia para funciones en Technical Preview, pero agradece comentarios para mejorarlas. Es posible que Citrix actúe a partir de los comentarios en función de su gravedad e importancia.

### Lista de funciones en Technical Preview

En esta tabla se enumeran las funciones en Technical Preview. Se trata de adelantos de funciones disponibles previa solicitud. Para habilitar cualquiera de estas funciones y enviar comentarios sobre las mismas, rellene los formularios correspondientes.

Título	Disponible a partir de la versión	Formulario de habilitación (haga clic en el icono)	Formulario de comentarios (haga clic en el icono)
<a href="#">Función disponible para aplicar autenticación biométrica para acceder a la aplicación Citrix Workspace</a>	2405		
<a href="#">Función disponible para inicio de sesión único para máquinas virtuales unidas a Microsoft Entra ID</a>	2405		
<a href="#">Función para configurar los parámetros de la aplicación Citrix Workspace a través de UEM</a>	24.3.5		
<a href="#">Función disponible para audio adaptativo</a>	24.3.0		
<a href="#">Compatibilidad con Accesibilidad y VoiceOver</a>	24.2.0		
<a href="#">Compatibilidad con cámaras web externas</a>	23.12.0		
<a href="#">Agregar varios almacenes mediante Unified Endpoint Management (UEM)</a>	23.9.0		

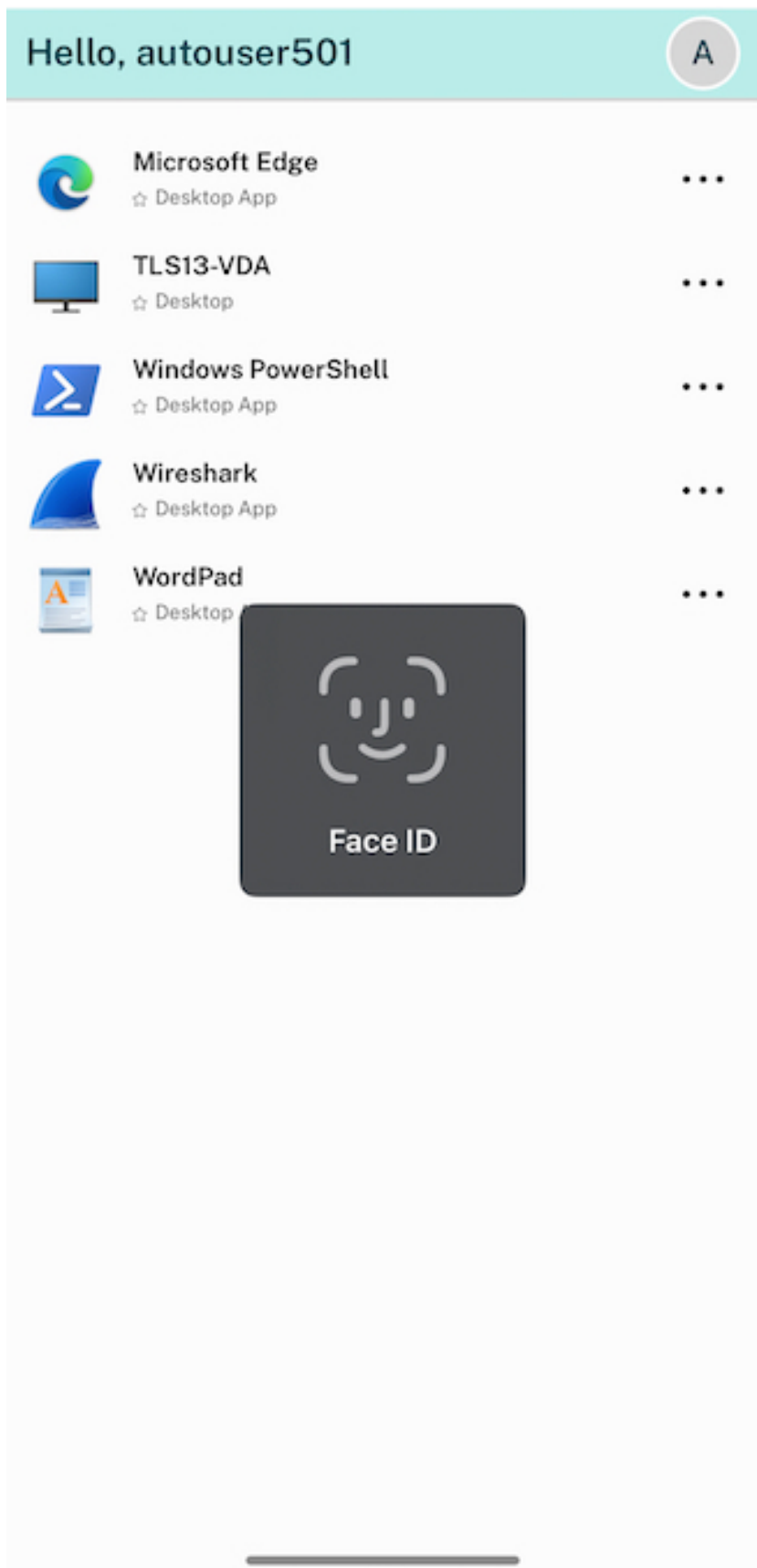
Título	Disponible a partir de la versión	Formulario de habilitación (haga clic en el icono)	Formulario de comentarios (haga clic en el icono)
<a href="#">Eliminar varios almacenes mediante Unified Endpoint Management (UEM)</a>	23.9.0		
<a href="#">Escaneo rápido</a>	23.3.5		
<a href="#">Compatibilidad con imágenes incrustadas (PiP)</a>	23.3.0		
<a href="#">Función disponible para el modo de no duplicación nativo de Apple</a>	23.3.0		
<a href="#">Compatibilidad con experiencia mejorada de Single Sign-On (SSO) para aplicaciones web y SaaS</a>	23.3.0		

### **Función disponible para aplicar autenticación biométrica para acceder a la aplicación Citrix Workspace**

Technical Preview a partir de la versión 2405 [Formulario de habilitación](#) [Formulario de comentarios](#)

A partir de la versión 24.5.0, ahora los administradores pueden imponer la autenticación biométrica de un dispositivo para que sus usuarios accedan a la aplicación Citrix Workspace. Con esta función, cuando abre la aplicación Citrix Workspace después de descartarla o la trae a primer plano después de minimizarla, se muestra una solicitud de verificación de Face ID o Touch ID para desbloquear e

iniciar sesión. Si el dispositivo no admite la autenticación biométrica, se utiliza el método de autenticación con contraseña o código de acceso para acceder a la aplicación. Si el código de acceso no está habilitado en el dispositivo, se cierra la sesión de la cuenta, lo que requiere que el usuario vuelva a iniciar sesión para acceder a la aplicación Citrix Workspace.



Los administradores pueden configurar esta función mediante la solución de administración unificada de dispositivos de punto final con los siguientes pares de valores clave:

- **clave:** `verify_biometric_on_app_foreground_transition`
- **tipo de valor:** booleano
- **valor:** true o false
  - Si se establece en **verdadero**, se requiere la autenticación biométrica para que los usuarios finales accedan a la aplicación Citrix Workspace.
  - Si se establece en **falso**, no se impone la autenticación biométrica para acceder a la aplicación Citrix Workspace. Los usuarios tienen la opción de inhabilitar la autenticación biométrica.

### **Función disponible para inicio de sesión único para máquinas virtuales unidas a Microsoft Entra ID**

---

Technical Preview a partir de la [Formulario de habilitación](#) [Formulario de comentarios](#)  
versión 2405

---

A partir de la versión 24.5.0, la aplicación Citrix Workspace para iOS permite a los usuarios iniciar sesión en dispositivos VM unidos a Azure AD mediante la autenticación de inicio de sesión único. Debe proporcionar las credenciales de Microsoft al iniciar sesión en un dispositivo de máquina virtual unido a Azure AD por primera vez. Para los inicios de sesión posteriores, no se requieren credenciales hasta que el token caduque.

#### **Nota:**

- Si el usuario no usa **WKwebview** para la autenticación, las credenciales se deben introducir por primera vez.
- Esta función solo se aplica a los almacenes de la nube.

### **Función para configurar los parámetros de la aplicación Citrix Workspace a través de UEM**

---

Technical Preview a partir de la [Formulario de habilitación](#) [Formulario de comentarios](#)  
versión 24.3.5

---

Anteriormente, solo se podía configurar la URL de almacén en la aplicación Citrix Workspace mediante Unified Endpoint Management (UEM).

A partir de la versión 24.3.5, también puede configurar los parámetros de la aplicación Citrix Workspace en los dispositivos administrados mediante cualquier solución de UEM que se implemente en su infraestructura.

**Nota:**

Como administrador, si tiene la opción de configurar los parámetros de la aplicación Citrix Workspace mediante UEM y Global App Configuration Service (GACS), UEM siempre tendrá prioridad sobre GACS.

A continuación, se muestra un archivo JSON de ejemplo para configurar los parámetros de la aplicación Citrix Workspace:

```
1 <dict>
2   <key>stores</key>
3   <array>
4     <dict>
5       <key>url</key>
6       <string>https://teststore.cloud.com</string>
7       <key>storeType</key>
8       <integer>1</integer>
9       <key>displayName</key>
10      <string>Cloud Store 1</string>
11      <key>appSettings</key>
12      <array>
13        <dict>
14          <key>category</key>
15          <string>audio</string>
16          <key>userOverride</key>
17          <false/>
18          <key>settings</key>
19          <array>
20            <dict>
21              <key>name</key>
22              <string>settings_audio_stream</string>
23              <key>value</key>
24              <true/>
25            </dict>
26          </array>
27        </dict>
28      <dict>
29        <key>category</key>
30        <string>authentication</string>
31        <key>userOverride</key>
32        <false/>
33        <key>settings</key>
34        <array>
35          <dict>
36            <key>name</key>
37            <string>settings_auth_web_browser</string>
38            <key>value</key>
39            <string>embedded</string>
```

```

40         </dict>
41     </array>
42 </dict>
43 </array>
44 </dict>
45 <dict>
46     <key>url</key>
47     <string>https://teststore.cloud.com</string>
48     <key>storeType</key>
49     <integer>1</integer>
50     <key>displayName</key>
51     <string>StoreFront1</string>
52     <key>appSettings</key>
53     <array>
54         <dict>
55             <key>category</key>
56             <string>audio</string>
57             <key>userOverride</key>
58             <false/>
59             <key>settings</key>
60             <array>
61                 <dict>
62                     <key>name</key>
63                     <string>settings_audio_stream</string>
64                     <key>value</key>
65                     <false/>
66                 </dict>
67             </array>
68         </dict>
69         <dict>
70             <key>category</key>
71             <string>authentication</string>
72             <key>userOverride</key>
73             <false/>
74             <key>settings</key>
75             <array>
76                 <dict>
77                     <key>name</key>
78                     <string>settings_auth_web_browser</string>
79                     <key>value</key>
80                     <string>system</string>
81                 </dict>
82             </array>
83         </dict>
84     </array>
85 </dict>
86 </array>
87 <key>storesToDelete</key>
88 <array>
89     <string>test.cldblr.com</string>
90     <string>test.cloud.com</string>
91 </array>
92 <key>restrict_user_store_modification</key>

```



```
93 <false/>
94 </dict>
95 <!--NeedCopy-->
```

**Nota:**

El indicador `userOverride` permite al usuario modificar los parámetros de la aplicación Citrix Workspace. Si el indicador `userOverride` se establece en `true`, el usuario puede cambiar los parámetros. Si el indicador `userOverride` se establece en `false` para algún parámetro, el usuario no podrá modificarlo en los parámetros de la aplicación Citrix Workspace.

**Tabla de pares clave-valor**

La siguiente tabla proporciona la información del par clave-valor:

**Nota:**

Los parámetros que sean específicos de una categoría debe agregarlos en un bloque de esa categoría.

Categoría	Parámetro	Descripción	Tecla	Valor	Tipo de valor	Valor predeterminado
audio	Audio	Proporciona acceso a los usuarios para activar o desactivar el audio desde la aplicación o el escritorio virtual.	settings_audio_trust	true/false	Booleano	TRUE
teclado	Usar teclado Unicode	Permite a los usuarios usar un teclado Unicode estándar.	settings_use_unicode_keyboard	true/false	Booleano	TRUE

Categoría	Parámetro	Descripción	Tecla	Valor	Tipo de valor	Valor predefinido
teclado	Teclado automático	Habilita o inhabilita la presentación automática del teclado en una sesión.	settings_automate_keyboard	true/false	Booleano	TRUE
teclado	Sincronización de la distribución del teclado	Permite a los usuarios cambiar a una distribución de teclado preferida en el dispositivo.	settings_keyboard_sync	true/false	Booleano	FALSE
teclado	Usar teclados personalizados	Permite a los usuarios usar teclados de terceros que se descargan en la sesión virtual.	settings_allow_third_party_keyboards	true/false	Booleano	FALSE
pantalla	Resolución de la sesión	Permite a los usuarios seleccionar la resolución de la pantalla.	settings_resolution	0-9	Número entero	5 (iPad) 3 (iPhone)

Categoría	Parámetro	Descripción	Tecla	Valor	Tipo de valor	Valor predefinido
pantalla	Modo de pre-presentación	Le permite usar su dispositivo iOS como panel táctil para controlar la sesión mientras usa una pantalla externa.	settings_presentation_mode	true/false	Booleano	FALSE
pantalla	Pantalla externa	Conecta una pantalla externa al dispositivo.	settings_external_display	true/false	Booleano	TRUE
avanzado	Validación estricta de certificados	Aplica un control más estricto en la validación de los certificados del servidor.	settings_strict_certificate_validation	true/false	Booleano	FALSE
avanzado	Versiones de TLS	Permite a los usuarios cambiar los parámetros de TLS para solucionar problemas.	settings_tlsVersion	0-3	Número entero	0

Categoría	Parámetro	Descripción	Tecla	Valor	Tipo de valor	Valor predefinido
avanzado	Usar cuadro combinado nativo	Permite el uso de la función de selección nativa de iOS.	settings_native_checkbox	true/false	Booleano	TRUE
avanzado	Uso táctil (solo iPad)	Habilita la función táctil en todas las aplicaciones y escritorios, incluidas las que no tienen la opción táctil habilitada de forma nativa.	settings_multitouch	true/false	Booleano	true (iPad) false (iPhone)
avanzado	Vista de pantalla completa	Le permite ver sus aplicaciones y escritorios en pantalla completa.	settings_mobile_fullscreen	true/false	Booleano	true (iPad) false (iPhone)

Categoría	Parámetro	Descripción	Tecla	Valor	Tipo de valor	Valor predefinido
avanzado	Reconectar al iniciar sesión	Permite que una sesión se vuelva a conectar automáticamente cuando se agrega una nueva cuenta o durante el inicio de sesión.	settings_reconnect_on_login	true/false	Booleano	FALSE
avanzado	Reconectar al actualizar	Se conecta de nuevo automáticamente a una sesión iniciada desde otro dispositivo al actualizar las aplicaciones o los escritorios del segundo dispositivo.	settings_reconnect_on_refresh	true/false	Booleano	FALSE
avanzado	Habilitar proxy HTTP	Le permite usar el proxy HTTP para una sesión.	settings_use_local_proxy	true/false	Booleano	TRUE

Categoría	Parámetro	Descripción	Tecla	Valor	Tipo de valor	Valor predefinido
avanzado	Usar credenciales derivadas	Permite usar credenciales derivadas.	setting_useDerivedCredentials	true/false	Booleano	FALSE
avanzado	Tarjeta inteligente en sesión	Permite el uso de un dispositivo de tarjeta inteligente dentro de una sesión. Este parámetro no permite a los usuarios autenticarse en la sesión.	settings_useSmartCardInsideSession	true/false	Booleano	FALSE
avanzado	Permitir EDT	Habilita el transporte adaptable.	settings_allowEDT	true/false	Booleano	TRUE
avanzado	Modo de tableta automático	Permite iniciar la sesión virtual en modo tableta cuando no se detecta ningún teclado o mouse externo.	settings_enableTabletModeSwitch	true/false	Booleano	TRUE
avanzado	Mantener pantalla activa	Mantener la pantalla encendida.	settings_stay_away	true/false	Booleano	FALSE

Categoría	Parámetro	Descripción	Tecla	Valor	Tipo de valor	Valor predefinido
avanzado	Usar el almacenamiento del iPad	Le permite acceder a las unidades locales de su dispositivo.	settings_clientdrive	true/false	Booleano	false
Mouse X1	Permitir el mouse X1	Le permite cambiar al mouse Citrix X1.	settings_allowX1	true/false	Booleano	FALSE
Mouse X1	Velocidad del mouse Citrix X1	Permite a los usuarios controlar la velocidad del cursor del mouse dentro de la sesión virtual.	settings_x1MouseSpeed	1-2	Número entero	200 (iPad Pro) 100 (todos los demás dispositivos)

Categoría	Parámetro	Descripción	Tecla	Valor	Tipo de valor	Valor predefinido
Mouse X1	Usar la imagen del cursor remoto para el mouse Citrix X1	Hace que el cursor se adapte a la aplicación o el escritorio de una sesión. Por ejemplo, si el cursor está sobre un cuadro de texto, cambia para adaptarse al cuadro de texto.	settings_X1_mouse/always_show_cursor	true/false	Booleano	TRUE
autenticación	Explorador web para autenticación	Le permite identificar el uso de SafariView-Controller en lugar de WKWeb en el dispositivo.	settings_auth_system/integrated	integrated	cadena	Integrado



thirdPartyServicesLaunchDarkly	Habilita el indicador de LaunchDarkly en las funciones de la aplicación Citrix Workspace.	enableLaunchDarkly	false	Booleano	true (regiones distintas de la UE)
--------------------------------	---	--------------------	-------	----------	------------------------------------

---

### **Función disponible para audio adaptativo**

---

Technical Preview a partir de la [Formulario de habilitación](#) [Formulario de comentarios](#)  
versión 24.3.0

---

A partir de la versión 24.3.0, la aplicación Citrix Workspace para iOS admite el audio adaptable HDX. Esta función mejora la experiencia del usuario al proporcionar calidad de audio mejorada y baja latencia.

Para obtener más información, consulte el artículo sobre [configuración de la directiva de audio](#) en la documentación de Citrix Virtual Apps and Desktops.

### **Compatibilidad con Accesibilidad y VoiceOver**

---

Technical Preview a partir de la [Formulario de habilitación](#) [Formulario de comentarios](#)  
versión 24.2.0

---

A partir de la versión 24.2.0, la aplicación Citrix Workspace para iOS admite las funciones Accesibilidad y VoiceOver. Esta función ayuda a los usuarios finales que tienen dificultades para ver la pantalla. El narrador lee los elementos de la pantalla en voz alta cuando se utiliza Citrix Workspace y la interfaz de usuario de sesiones virtuales.

Para habilitar la función VoiceOver, vaya a **Ajustes > Accesibilidad > VoiceOver** de iOS y actívela.

Debe utilizar los gestos estándar de accesibilidad que proporciona iOS para interactuar con la aplicación Citrix Workspace. Por ejemplo, puede deslizar el dedo hacia la izquierda y hacia la derecha en la pantalla para navegar entre los menús mientras se reproduce la voz en off para cada elemento.

Para obtener más información, consulte [Introducción a las funciones de accesibilidad del iPhone](#) e [Introducción a las funciones de accesibilidad del iPad](#) en la documentación de asistencia técnica de Apple.

## Compatibilidad con cámaras web externas

---

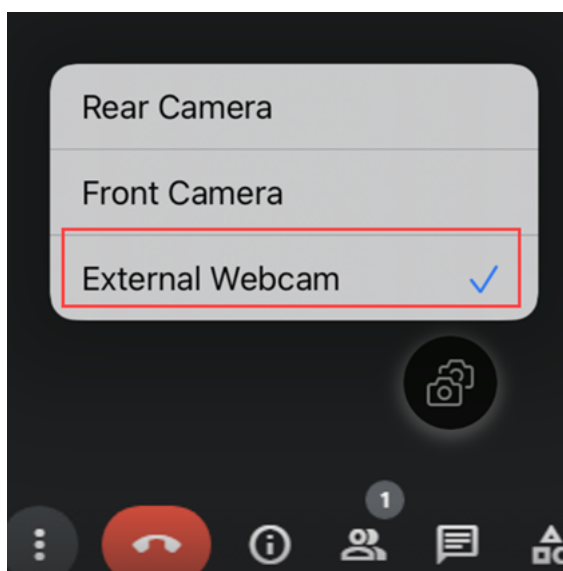
Technical Preview a partir de la [Formulario de habilitación](#) [Formulario de comentarios](#)  
versión 23.12.0

---

La aplicación Citrix Workspace para iOS ahora es compatible con cámaras web conectadas externamente dentro de las sesiones de DaaS. Conecte una cámara web mediante USB y utilícela para realizar videoconferencias haciendo clic en el icono de la cámara y, a continuación, seleccionando la opción **Cámara web externa**. Mejora la experiencia en las sesiones al aprovechar los recursos disponibles para los usuarios finales.

### Nota:

- La cámara web externa solo es compatible con iPads con iOS 17 o versiones posteriores con un conector USB-C.
- La opción Cámara web externa solo aparece cuando se detecta una cámara externa.
- Los parámetros de la aplicación cliente no afectan a la cámara durante una sesión HDX. Debe usar el botón flotante de la cámara que Citrix habilita para cambiar la posición de la cámara.



La próxima vez que use una aplicación de videoconferencia, el sistema recordará sus preferencias y utilizará la preferencia de cámara en consecuencia. Por ejemplo, si finalizaste la última videollamada

con la preferencia **Cámara web externa**, la próxima vez la cámara web externa estará seleccionada de forma predeterminada.

Para cambiar las preferencias de la cámara, toque el icono de la cámara en la pantalla. También puede cambiar las preferencias de la cámara durante las llamadas.

Esta función está disponible para los clientes de almacenes locales y de la nube.

## Agregar varios almacenes mediante Unified Endpoint Management (UEM)

---

Technical Preview a partir de la [Formulario de habilitación](#) [Formulario de comentarios](#)  
versión 23.12.0

---

Los administradores pueden usar las soluciones de Unified Endpoint Management (UEM) para configurar y agregar varios almacenes para los dispositivos iOS administrados. Los detalles de cada almacén se pueden agregar a un archivo XML. A continuación, este archivo XML se puede cargar mientras se configura la directiva de configuración de aplicaciones.

**Nota:**

El archivo XML debe estar en formato clave-valor.

---

Clave de configuración	Tipo de valor	Descripción
url	Cadena	La URL del almacén. Por ejemplo, ejemplo.cloud.com
storeType (opcional)	Número entero	Si se establece en <b>1</b> , los usuarios pueden ver la carga nativa o predeterminada del almacén. Si se establece en <b>2</b> , los usuarios pueden ver el almacén dentro de una interfaz web.
displayName (opcional)	Cadena	El nombre del almacén.

Clave de configuración	Tipo de valor	Descripción
restrict_user_store_modification (opcional)	Booleano	Si se establece en <b>true</b> , los usuarios no pueden hacer cambios; es decir, ni agregar ni eliminar ni modificar el almacén. Si se establece en <b>false</b> , los usuarios pueden hacer cambios; es decir, pueden agregar, eliminar y modificar el almacén.

### Importante

- Si el indicador **restrict\_user\_store\_modification** se establece en **true**, todos los almacenes existentes se eliminan antes de agregar un nuevo almacén configurado para UEM.
- Si no se proporciona storeType, la interfaz predeterminada se considera nativa.

### Ejemplo de configuración XML para agregar almacenes

Consulte este archivo XML de ejemplo para obtener más información.

```

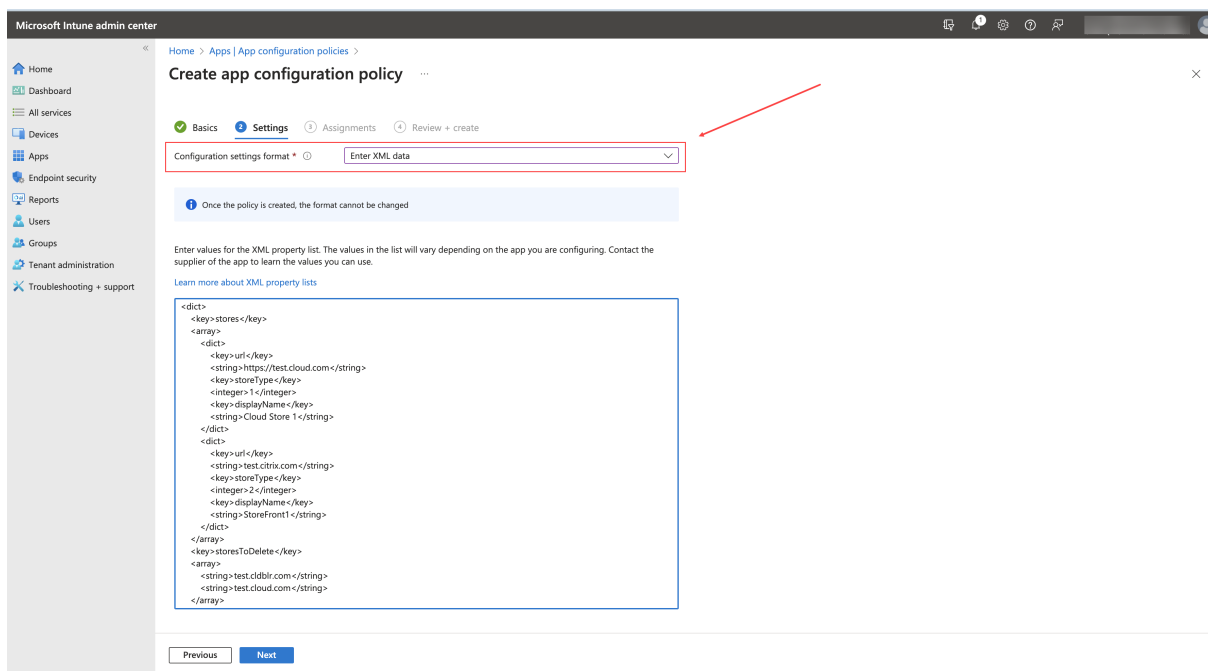
1     <dict>
2         <key>stores</key>
3         <array>
4             <dict>
5                 <key>url</key>
6                 <string>test.cloud.com</string>
7                 <key>storeType</key>
8                 <integer>1</integer>
9                 <key>displayName</key>
10                <string>Cloud Store </string>
11            </dict>
12            <dict>
13                <key>url</key>
14                <string>test.citrix.com</string>
15                <key>storeType</key>
16                <integer>2</integer>
17                <key>displayName</key>
18                <string>StoreFront</string>
19            </dict>
20        </array>
21        <key>restrict_user_store_modification</key>
22        <true/>
23    </dict>

```

24

25 <!--NeedCopy-->

Cuando el archivo XML esté listo con la configuración del almacén, los administradores pueden cargar el archivo en la página **Crear directiva de configuración de aplicaciones**. Por ejemplo, en Microsoft Intune, los administradores deben seleccionar la opción **Introducir datos xml** del menú desplegable **Formato de los parámetros de configuración**.



## Eliminar varios almacenes mediante Unified Endpoint Management (UEM)

Technical Preview a partir de la [Formulario de habilitación](#) [Formulario de comentarios](#)  
versión 23.12.0

Los administradores deben agregar una lista de los almacenes que se eliminarán a un archivo XML con el nombre clave **storesToDelete** para eliminar uno o más almacenes.

### Ejemplo de configuración XML para eliminar almacenes

Consulte este archivo XML de ejemplo para obtener más información.

```
1 <dict>
2   <key>storesToDelete</key>
3   <array>
4     <string>test.cldblr.com</string>
```

```
5     <string>test.onprem.com</string>
6   </array>
7 </dict>
8
9 <!--NeedCopy-->
```

A continuación se muestra un ejemplo de archivo de configuración XML que contiene la configuración para agregar y eliminar almacenes.

```
1     <dict>
2       <key>stores</key>
3       <array>
4         <dict>
5           <key>url</key>
6           <string>test.cloud.com</string>
7           <key>storeType</key>
8           <integer>1</integer>
9           <key>displayName</key>
10          <string>Cloud Store </string>
11        </dict>
12        <dict>
13          <key>url</key>
14          <string>test.citrix.com</string>
15          <key>storeType</key>
16          <integer>2</integer>
17          <key>displayName</key>
18          <string>StoreFront</string>
19        </dict>
20      </array>
21      <key>storesToDelete</key>
22      <array>
23        <string>test.cldblr.com</string>
24        <string>test.onprem.com</string>
25      </array>
26      <key>restrict_user_store_modification</key>
27      <true/>
28    </dict>
29
30 <!--NeedCopy-->
```

## Escaneo rápido

---

Technical Preview a partir de la [Formulario de habilitación](#) [Formulario de comentarios](#)  
versión 23.3.5

---

Si ha iniciado sesión en la aplicación Citrix Workspace desde varios dispositivos, puede usar la función de escaneo rápido para escanear varios documentos con un dispositivo iOS. A continuación, transfiera esos documentos escaneados a un dispositivo iOS.

Para obtener instrucciones sobre cómo utilizar la función de escaneo rápido para escanear documentos, siga estos pasos:

1. En su dispositivo Mac, haga clic con el botón derecho en el icono de la aplicación Citrix Workspace de la sesión de escritorio y haga clic en **Escaneo rápido**. Se mostrará un código QR.
2. En su dispositivo iOS, haga clic en **Ajustes > Escaneo rápido**.
3. Escanee el código QR que aparece en su dispositivo Mac para establecer la conexión entre su Mac y los dispositivos iOS.
4. Escanee los documentos que quiera y envíelos a su dispositivo Mac.
5. En la sesión de escritorio de su dispositivo Mac, puede buscar los documentos escaneados en el Finder.

### Requisitos previos

- La asignación de unidades del cliente (CDM) debe estar habilitada para el almacén.
- Debe iniciar sesión con la misma cuenta en la aplicación Citrix Workspace, tanto en el dispositivo iOS como en el dispositivo Mac.
- Debe conectarse a la misma red Wi-Fi.
- La versión mínima requerida de la aplicación Citrix Workspace para Mac es la 2304.
- El escaneo rápido requiere acceso de lectura y escritura en el dispositivo. Para habilitar el acceso, siga estos pasos:
  1. Desde su perfil, haga clic en **Parámetros de aplicación > Parámetros de almacén**.
  2. Haga clic en su almacén actual.
  3. Haga clic en **Almacenamiento del dispositivo** y seleccione **Acceso de lectura y escritura**.

### Compatibilidad con imágenes incrustadas (PiP)

---

Technical Preview a partir de la [Formulario de habilitación](#) [Formulario de comentarios](#)  
versión 23.3.0

---

La aplicación Citrix Workspace para iOS admite el modo de imagen incrustada (PiP), lo que le permite reducir el tamaño de las sesiones de escritorio, las aplicaciones SaaS o las aplicaciones web a ventanas flotantes. Puede mover esta ventana libremente por la pantalla y colocarla en cualquier lugar. El modo PiP libera la pantalla de inicio de la aplicación Citrix Workspace para que pueda completar otras tareas. Haga clic en el botón **Inicio** de la barra de herramientas de la sesión de su sesión de escritorio o en el **menú de puntos suspensivos (...)** > **Minimizar** de su aplicación SaaS o web para minimizar la pantalla. Haga clic en la ventana flotante para ver la aplicación en pantalla completa y

ciérrela con el icono **X** de la ventana flotante. La ventana flotante aparece automáticamente en pantalla completa al minimizar otra aplicación.

Esta función es compatible con las implementaciones locales y de la nube. Sin embargo, para las implementaciones de la nube, las aplicaciones web se pueden minimizar a una imagen incrustada. Para cambiar entre una sesión de escritorio y una aplicación web, también puede hacer clic en la ventana flotante.

**Nota:**

Solo puede mantener dos aplicaciones activas a la vez. Una en modo de pantalla completa y la otra minimizada como imagen incrustada:

- 2 aplicaciones web o SaaS
- 1 aplicación web o SaaS y 1 sesión de escritorio o aplicación virtual

**Limitaciones conocidas:**

- El modo PiP no está disponible cuando se conectan periféricos externos, como un mouse, un teclado o un monitor externo.
- Si el modo PiP está habilitado y el dispositivo está conectado a un monitor externo, la aplicación Citrix Workspace no responde y el botón de retroceso no está disponible en **Parámetros de pantalla** de la sesión de escritorio.

### **Función para el modo de no duplicación nativo de Apple**

---

Technical Preview a partir de la [Formulario de habilitación](#) [Formulario de comentarios](#)  
versión 22.12.0

---

Ahora puede prolongar la pantalla con el modo de no duplicación de Apple, disponible con iPad OS 16.2. Puede realizar varias tareas a la vez con la aplicación Citrix Workspace, aplicaciones virtuales y escritorios virtuales en el monitor externo y con la pantalla del iPad libre para ejecutar otras aplicaciones nativas.

**Nota:**

La función de pantalla prolongada en el modo de no duplicación de Apple solo está disponible en algunos modelos de iPad. Para obtener más información, consulte la [documentación de Apple](#).

Si no quiere utilizar esta función en Technical Preview, siempre puede utilizar la aplicación Citrix Workspace en el modo de pantalla completa.



## Compatibilidad con experiencia mejorada de Single Sign-On (SSO) para aplicaciones web y SaaS

---

Technical Preview a partir de la [Formulario de habilitación](#) [Formulario de comentarios](#)  
versión 22.3.5

---

Esta función simplifica la configuración de SSO para aplicaciones web y SaaS internas al usar proveedores de identidades (IdP) de terceros. La experiencia mejorada de SSO reduce todo el proceso a unos pocos comandos. Elimina el requisito previo obligatorio de configurar Citrix Secure Private Access en la cadena de IdP para configurar SSO. También mejora la experiencia del usuario, siempre que se utilice el mismo IdP para la autenticación tanto en la aplicación Workspace como en la aplicación web o SaaS correspondiente que se inicie.

### De la versión Technical Preview a la versión de disponibilidad general (GA)

---

Servicio o función	Versión de disponibilidad general
<a href="#">Función disponible para escáner de documentos</a>	24.5.0
<a href="#">Compatibilidad con autenticación basada en FIDO2</a>	23.9.0

---

## Requisitos del sistema y compatibilidad

March 28, 2024

### Requisitos de dispositivo

- La versión 23.9.0 de la aplicación Citrix Workspace para iOS y versiones posteriores son compatibles con iOS 17 y iPadOS 17.
- La versión 22.9.0 de la aplicación Citrix Workspace para iOS y versiones posteriores son compatibles con iOS 16 y iPadOS 16.
- La versión 21.9.1 de la aplicación Citrix Workspace para iOS y versiones posteriores son compatibles con iOS 15 y iPadOS 15.
- La versión 20.9.0 de la aplicación Citrix Workspace para iOS y versiones posteriores son compatibles con iOS 14 y iPadOS 14.

- Esta actualización de software ha sido validada en los dispositivos siguientes:
  - Modelos iPhone 7x, modelos iPhone 8x y solo el modelo iPhone X.
  - Todos los modelos de iPad (incluido iPad Pro) con la excepción del iPad 1 y el iPad 2, que no son compatibles.
- Funcionalidad de presentación en pantallas externas
  - iPhone: Lo compatible con iOS.
  - iPad: Lo compatible con iOS (no usa toda la pantalla).

### Requisitos del servidor

Compruebe que ha instalado todas las revisiones hotfix más recientes en los servidores.

- Para conexiones con aplicaciones y escritorios virtuales, la aplicación Citrix Workspace es compatible con Citrix StoreFront y la Interfaz Web.

StoreFront:

- StoreFront 3.6 o versiones posteriores (recomendado). La aplicación Citrix Workspace ha sido validada con la versión más reciente de StoreFront; entre las versiones anteriores compatibles están StoreFront 2.6 y posteriores.

Ofrece acceso directo a almacenes de StoreFront. La aplicación Citrix Workspace también es compatible con versiones anteriores de StoreFront.

**Nota:**

Con XenApp y XenDesktop 7.8, Citrix introdujo el canal virtual Framehawk y 3D Pro. Esta funcionalidad se amplió a la aplicación Citrix Workspace.

- StoreFront configurado con Workspace para sitios web.

Da acceso a los almacenes de StoreFront a través de un explorador web Safari. Los usuarios deben abrir manualmente el archivo ICA con el explorador web. Para conocer las limitaciones de esta implementación, consulte la documentación de [StoreFront](#).

Interfaz Web:

- Interfaz Web 5.4 con sitios de Interfaz Web
- Interfaz Web 5.4 con sitios de XenApp y XenDesktop
- Interfaz Web en Citrix Gateway (solo acceso basado en explorador web con Safari)

Habilite las directivas de reescritura proporcionadas por Citrix Gateway.

- **Citrix Virtual Apps and Desktops, XenApp y XenDesktop** (cualquiera de los siguientes productos):
  - Citrix Virtual Apps and Desktops 7 1808 o versiones posteriores.
  - Citrix XenDesktop 7.x o versiones posteriores
  - Citrix XenApp 7.5 o versiones posteriores

### Conexiones, certificados y autenticación

Para conexiones con StoreFront, la aplicación Citrix Workspace admite los siguientes métodos de autenticación:

	Workspace para Web con exploradores web	Sitio de servicios de StoreFront (nativo)	Sitio de XenApp y XenDesktop de StoreFront (nativo)	De Citrix Gateway a Workspace para Web (explorador web)	Citrix Gateway en el sitio de StoreFront Services (nativo)
Anónimo	Sí	Sí			
Dominio	Sí	Sí	Sí	Sí*	Sí*
PassThrough de dominio	Sí	Sí	Sí		
Token de seguridad				Sí*	Sí*
Autenticación de dos factores (dominio con token de seguridad)				Sí*	Sí*
SMS				Sí*	No
Tarjeta inteligente		Sí		Sí*	Sí*
Certificado de usuario				Sí (plug-in de Citrix Gateway)	Sí (plug-in de Citrix Gateway)

\*Disponible solo para:

- Workspace para sitios web.
- Implementaciones que incluyen Citrix Gateway, con o sin el plug-in asociado instalado en el dispositivo.

**Nota:**

El plug-in del análisis de punto final (EPA) de Citrix Gateway está disponible en Citrix Workspace. En la aplicación nativa de Citrix Workspace, solo está disponible cuando se usa la autenticación nFactor. Para obtener más información, consulte [Configure pre-auth and post-auth EPA scan as a factor in nFactor authentication](#) en la documentación de Citrix ADC.

Para conexiones con la Interfaz Web 5.4, la aplicación Citrix Workspace admite los siguientes métodos de autenticación:

**Nota:**

La Interfaz Web usa el término “Explícita” para la autenticación con dominio y token de seguridad.

	Interfaz Web (exploradores web)	Sitio de XenDesktop y XenApp de Interfaz Web	De Citrix Gateway a la Interfaz Web (explorador web)	Citrix Gateway en el sitio de XenApp y XenDesktop de Interfaz Web
Anónimo	Sí			
Dominio	Sí	Sí	Sí*	
PassThrough de dominio	Sí			
Token de seguridad			Sí*	
Autenticación de dos factores (dominio con token de seguridad)			Sí*	
SMS			Sí*	
Tarjeta inteligente				
Certificado de usuario			Sí (requiere el plug-in de Citrix Gateway)	

## Certificados

**Certificados privados (autofirmados)** Puede acceder a los recursos de Citrix mediante la aplicación Citrix Workspace:

- Cuando se instala un certificado privado en la puerta de enlace remota.
- Cuando el certificado raíz de la entidad de certificación de la organización está instalado en el dispositivo.

### Nota:

Cuando el certificado de la puerta de enlace remota no se puede verificar durante la conexión, aparece una advertencia de certificado que no es de confianza. Este problema se debe a que el certificado raíz no está incluido en el almacén de claves local. Si un usuario elige ignorar la advertencia y continuar con la conexión, se mostrará la lista de aplicaciones, pero no se podrán iniciar.

**Certificado instalado de forma manual** En iOS 10.3 y versiones posteriores, SSL no confía automáticamente en un certificado que esté incluido en un perfil e instalado de forma manual. Para confiar en perfiles de certificados instalados de forma manual en iOS:

1. Asegúrese de haber instalado el perfil de certificado en el dispositivo.
2. Vaya a **Ajustes > General > Información > Ajustes de confianza de los certificados**.

Cada raíz que se haya instalado mediante un perfil aparecerá en **Confiar en los certificados raíz**.

3. Puede habilitar o inhabilitar la confianza para cada certificado raíz.

**Importación de certificados raíz en dispositivos iPhone y iPad** Obtenga el certificado raíz de la entidad de certificación y envíelo por correo electrónico a una cuenta de correo electrónico configurada en el dispositivo. Al seleccionar el adjunto, se le pedirá que importe el certificado raíz.

**Certificados comodín** Se usan certificados comodín en lugar de los certificados de servidor individuales para cualquier servidor dentro del mismo dominio. La aplicación Citrix Workspace admite certificados comodín.

**Certificados intermedios y Citrix Gateway** Cuando la cadena de certificados incluye un certificado intermedio, es necesario añadir ese certificado intermedio al certificado de servidor de Citrix Gateway (o Access Gateway). Además, para las instalaciones de Access Gateway, consulte el artículo

[Instalar, vincular y actualizar certificados](#) que se ajusten a sus requisitos en la documentación de Citrix ADC.

La autenticación con RSA SecurID es compatible con las configuraciones de Secure Gateway (mediante la Interfaz Web solamente) y todas las configuraciones de Access Gateway admitidas.

La aplicación Citrix Workspace admite todos los métodos de autenticación compatibles con Access Gateway.

**Directiva de validación conjunta de certificados de servidor** Las versiones de la aplicación Citrix Workspace presentan una directiva más estricta para validar los certificados de servidor.

#### Importante

Antes de instalar la aplicación Citrix Workspace, confirme que los certificados presentes en el servidor o la puerta de enlace se hayan configurado correctamente como se describe aquí. Las conexiones pueden fallar si:

- La configuración del servidor o la puerta de enlace incluye un certificado raíz incorrecto
- La configuración del servidor o la puerta de enlace no incluye todos los certificados intermedios
- La configuración del servidor o la puerta de enlace incluye un certificado intermedio caducado o no válido
- La configuración del servidor o la puerta de enlace incluye un certificado intermedio con firmas cruzadas

Ahora, cuando valida un certificado de servidor, la aplicación Citrix Workspace usa **todos** los certificados suministrados por el servidor (o la puerta de enlace) para validarlo. Al igual que en las versiones anteriores, esta versión de la aplicación Citrix Workspace también comprueba posteriormente que los certificados son de confianza. Si no los certificados son de confianza, la conexión falla.

Esta directiva es más estricta que la directiva de certificados presente en los exploradores web. Muchos exploradores web incluyen un gran conjunto de certificados raíz en los que confían.

El servidor (o la puerta de enlace) debe estar configurado con el conjunto correcto de certificados. Un conjunto incorrecto de certificados puede provocar que fallen las conexiones de la aplicación Citrix Workspace.

Supongamos que se configura una puerta de enlace con estos certificados válidos. Esta configuración se recomienda para los clientes que requieren una validación más estricta, que necesitan determinar exactamente cuál es el certificado raíz usa la aplicación Citrix Workspace:

- Ejemplo de certificado de servidor
- Ejemplo de certificado intermedio
- Ejemplo de certificado raíz

A continuación, la aplicación Citrix Workspace comprueba que todos los certificados sean válidos. La aplicación Citrix Workspace también valida si el **Certificado raíz de ejemplo** ya es de confianza.

### Notas:

- Si la aplicación Citrix Workspace no confía en **Certificado raíz de ejemplo**, la conexión falla.
- Algunas entidades de certificación tienen más de un certificado raíz. Si necesita usar una validación más estricta, compruebe que la configuración usa el certificado raíz correspondiente.

Por ejemplo, actualmente hay dos certificados:

- DigiCert o GTE CyberTrust Global Root
- DigiCert Baltimore Root o Baltimore CyberTrust Root

Estos certificados pueden validar los mismos certificados de servidor. En algunos dispositivos de usuario, están disponibles ambos certificados raíz. En otros dispositivos, solo uno está disponible (**DigiCert Baltimore Root** o **Baltimore CyberTrust Root**).

Si configura **GTE CyberTrust Global Root** en la puerta de enlace, fallan las conexiones de la aplicación Citrix Workspace en esos dispositivos de usuario. Consulte la documentación de la entidad de certificación para determinar qué certificado raíz debe usarse. Tenga en cuenta que los certificados raíz también caducan, como todos los demás certificados.

A continuación, la aplicación Citrix Workspace usa estos dos certificados. La aplicación busca un certificado raíz en el dispositivo del usuario. Si encuentra uno que se valida correctamente y también es de confianza (por ejemplo, **Ejemplo de certificado raíz**), la conexión se realiza correctamente. De lo contrario, la conexión falla.

Esta configuración proporciona el certificado intermedio que necesita la aplicación Citrix Workspace, pero también permite que la aplicación Citrix Workspace elija cualquier certificado raíz válido y de confianza.

Supongamos ahora que se configura una puerta de enlace con estos certificados:

- Ejemplo de certificado de servidor
- Ejemplo de certificado intermedio
- Certificado raíz incorrecto

Un explorador web podría ignorar el certificado raíz incorrecto. No obstante, la aplicación Citrix Workspace no ignora el certificado raíz incorrecto y la conexión falla.

Algunas entidades de certificación usan más de un certificado intermedio. En este caso, la puerta de enlace se configura normalmente con todos los certificados intermedios (pero sin el certificado raíz):

- Ejemplo de certificado de servidor
- Ejemplo de certificado intermedio 1
- Ejemplo de certificado intermedio 2

### Importante

Algunas entidades de certificación usan un certificado intermedio con firmas cruzadas. Estos certificados están pensados para situaciones en que hay más de un certificado raíz y un certificado raíz anterior se usa al mismo tiempo que un certificado raíz posterior. En tales casos, existen al menos dos certificados intermedios.

Por ejemplo, el certificado raíz anterior **Class 3 Public Primary Certification Authority** tiene el certificado intermedio correspondiente de firmas cruzadas **Verisign Class 3 Public Primary Certification Authority - G5**. No obstante, un certificado raíz posterior correspondiente **Verisign Class 3 Public Primary Certification Authority - G5** también está disponible y reemplaza a **Class 3 Public Primary Certification Authority**. El certificado raíz posterior no usa ningún certificado intermedio con firmas cruzadas.

### Nota:

El certificado intermedio con firmas cruzadas y el certificado raíz tienen el mismo nombre de sujeto (Emitido para), pero el certificado intermedio con firmas cruzadas tiene un nombre de emisor diferente (Emitido por). El nombre de emisor distingue el certificado intermedio con firmas cruzadas de un certificado intermedio normal (como **Certificado intermedio 2 - ejemplo**).

Esta configuración, sin certificado raíz y sin certificado intermedio con firmas cruzadas, es la que se suele recomendar:

- Ejemplo de certificado de servidor
- Ejemplo de certificado intermedio

No configure la puerta de enlace para que use el certificado intermedio con firmas cruzadas, porque la aplicación Citrix Workspace seleccionará el certificado raíz anterior:

- Ejemplo de certificado de servidor
- Ejemplo de certificado intermedio
- Ejemplo de certificado intermedio con firmas cruzadas [no recomendado]

No se recomienda configurar la puerta de enlace solamente con el certificado del servidor:

- Ejemplo de certificado de servidor

En tales casos, si la aplicación Citrix Workspace no puede localizar todos los certificados intermedios, la conexión falla.



## Instalación y actualización

November 8, 2023

Puede descargar o actualizar a la versión más reciente de la aplicación Citrix Workspace desde el Apple Store.

- Los nuevos usuarios vez pueden descargar la aplicación Citrix Workspace desde el [Apple Store](#) e instalarla en sus dispositivos.
- Los usuarios existentes pueden actualizar a la versión más reciente de la aplicación Citrix Workspace desde el [Apple Store](#).

Para obtener información sobre cómo configurar la aplicación Citrix Workspace, consulte la sección [Configurar](#).

Para obtener información sobre las funciones disponibles en la aplicación Citrix Workspace para iOS, consulte [Tabla de funciones de la aplicación Citrix Workspace](#).

## Introducción

March 28, 2024

### Configurar

La aplicación Citrix Workspace para iOS admite la configuración de la Interfaz Web para la implementación de Citrix Virtual Apps. Hay dos tipos de sitios de Interfaz Web:

- Sitios de XenApp y XenDesktop
- Sitios de Citrix Virtual Apps and Desktops y Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service).

Los sitios de la Interfaz Web permiten a los dispositivos cliente conectarse con la comunidad de servidores. La autenticación entre la aplicación Citrix Workspace para iOS y el sitio de la Interfaz Web se puede gestionar mediante una variedad de soluciones, incluido Citrix Secure Web Gateway.

Además, se puede configurar StoreFront para proporcionar servicios de autenticación y entrega de recursos para la aplicación Citrix Workspace, lo que permite crear almacenes empresariales para la entrega de escritorios, aplicaciones y otros recursos para los usuarios.

Para obtener más información sobre cómo configurar las conexiones, incluidos vídeos, blogs y foros de asistencia, consulte <http://community.citrix.com>.

Para que los usuarios puedan acceder a las aplicaciones alojadas en la implementación de Citrix Virtual Apps and Desktops y Citrix DaaS, antes hay que configurar los componentes siguientes en el entorno como se describe a continuación.

- Cuando publique aplicaciones en comunidades o sitios, tenga en cuenta las siguientes opciones para mejorar la experiencia de los usuarios que acceden a esas aplicaciones a través de almacenes de StoreFront.
  - Incluya descripciones significativas para las aplicaciones publicadas, dado que estas descripciones estarán visibles para los usuarios de la aplicación Citrix Workspace.
  - Puede destacar ciertas aplicaciones publicadas para los usuarios de los dispositivos móviles, e incluirlas en la lista de Destacadas. Para rellenar esta lista en la aplicación Citrix Workspace, modifique las propiedades de las aplicaciones publicadas en los servidores. Ahora puede agregar la cadena “KEYWORDS: Featured” al valor del campo **Descripción de la aplicación**.
  - El modo de ajuste de pantalla ajusta la aplicación al tamaño de la pantalla de los dispositivos móviles. Para habilitar este modo, modifique las propiedades de las aplicaciones publicadas en los servidores y agregue la cadena de texto “KEYWORDS: mobile” en el valor del campo Descripción de la aplicación. Esta palabra clave también activa la función de desplazamiento automático para la aplicación.
  - Para suscribir automáticamente a todos los usuarios de un almacén a una aplicación, agregue la cadena “KEYWORDS: Auto” a la descripción cuando publique la aplicación en Citrix Virtual Apps. Cuando los usuarios inicien sesión en el almacén, la aplicación se aprovisionará automáticamente sin que los usuarios tengan que suscribirse de forma manual a la aplicación.
- Si la Interfaz Web de la implementación de Citrix Virtual Apps and Desktops y Citrix DaaS no tiene un sitio, cree uno. El nombre del sitio y la forma de crearlo depende de la versión de la Interfaz Web que tenga instalada.

### Configuración manual

En general, cuando la aplicación Citrix Workspace se conecta con Citrix Gateway, intenta encontrar un sitio de XenApp y XenDesktop o un sitio web de Citrix Virtual Apps después de la autenticación. Si no se detecta ningún sitio, la aplicación Citrix Workspace para iOS muestra un error. Para evitar esta situación, puede configurar manualmente una cuenta de modo que la aplicación Citrix Workspace para iOS pueda conectar con Citrix Gateway.

1. Toque el icono **Cuentas > pantalla Cuentas > signo más (+)**. Aparecerá la pantalla Nueva cuenta.
2. En la parte inferior izquierda de la pantalla, toque el icono a la izquierda de **Opciones** y luego en **Configuración manual**. Aparecerán otros campos en la pantalla.

3. En el campo **Dirección**, introduzca la dirección URL segura del sitio o Citrix Gateway (por ejemplo, [agee.mycompany.com](https://agee.mycompany.com)).
4. Seleccione alguna de estas opciones de conexión. Los otros campos de la pantalla cambiarán según lo que seleccione.
  - **Interfaz Web:** Seleccione si la aplicación Citrix Workspace mostrará un sitio web de Citrix Virtual Apps, similar a un explorador web. Esta interfaz de usuario se conoce como vista web.
  - **Servicios XenApp:** Esta opción permite a la aplicación Citrix Workspace para iOS encontrar un sitio de XenApp y XenDesktop concreto que no tenga configurada la autenticación mediante Citrix Gateway. En las opciones adicionales que aparecerán en la pantalla, introduzca las credenciales de inicio de sesión para el sitio.
    - `\<FQDN de StoreFront\>`: Si hay muchos almacenes, se presenta una lista al usuario para que elija el que quiere agregar.
    - `\<FQDN de StoreFront\>/citrix/\<Nombre de almacén\>`: Esta opción agrega el almacén de StoreFront `\<Nombre de almacén\>`.
    - `\<FQDN de StoreFront\>/citrix/PnAgent/config.xml`: Esta opción agrega el antiguo almacén predeterminado de PNAgent.
    - `\<FQDN de StoreFront\>/citrix/\<Nombre de almacén\>/PnAgent/config.xml`: Esta opción agrega el antiguo almacén PNAgent asociado a `\<Nombre de almacén\>`.
  - **Citrix Gateway:** Esta opción permite a la aplicación Citrix Workspace para iOS conectar con un sitio de XenApp y XenDesktop mediante un dispositivo Citrix Gateway concreto. En las opciones adicionales de esta pantalla, seleccione la edición del servidor y sus credenciales de inicio de sesión, y si requiere un token de seguridad para la autenticación.
5. Para el certificado de seguridad, use el parámetro del campo Ignorar advertencias de certificados para determinar si quiere conectar con el servidor, aunque este tenga un certificado no válido, autofirmado o caducado. De forma predeterminada, está desactivado.

Importante: Si decide habilitar esta opción, compruebe que se conecta al servidor correcto. Citrix recomienda encarecidamente que todos los servidores tengan un certificado válido para proteger a los dispositivos de usuario contra posibles ataques a la seguridad. Un servidor seguro usa un certificado SSL emitido por una entidad de certificación. Citrix no admite certificados autofirmados y no recomienda ignorar la seguridad de certificados.
6. Toque Guardar.
7. Introduzca su nombre de usuario y su contraseña (o token, si seleccionó la autenticación de dos factores), y toque Inicio de sesión. Aparecerá la pantalla de la aplicación Citrix Workspace para iOS, desde la cual puede acceder a sus escritorios, así como agregar y abrir aplicaciones.

## StoreFront

### Importante:

- Cuando se usa StoreFront, la aplicación Citrix Workspace para iOS es compatible con las versiones de Citrix Access Gateway Enterprise Edition a partir de la 9.3, y las versiones de Citrix Gateway hasta la 13.
- La aplicación Citrix Workspace para iOS solo ofrece soporte para sitios de XenApp y XenDesktop en la Interfaz Web.
- La aplicación Citrix Workspace para iOS admite el lanzamiento de sesiones desde Workspace para Web, siempre que el explorador web que se utilice funcione con Workspace para Web. Si no puede iniciar sesiones, configure su cuenta a través de la aplicación Citrix Workspace para iOS directamente. Los usuarios deben abrir manualmente el archivo ICA con la función Abrir en Workspace del explorador web. Para conocer las limitaciones de esta implementación, consulte la documentación de [StoreFront](#).

Con StoreFront, los almacenes que se crean consisten en servicios que proporcionan una infraestructura de recursos y autenticación para la aplicación Citrix Workspace para iOS. Cree almacenes que hagan recuento y sumen escritorios y aplicaciones de lo siguiente:

- Sitios de Citrix Virtual Apps and Desktops y Citrix DaaS
  - Comunidades de Citrix Virtual Apps
1. Instale y configure StoreFront. Para obtener información detallada, consulte la documentación de producto de [StoreFront](#). Para los administradores que necesitan más control, Citrix ofrece una plantilla que se puede usar para crear un sitio de descargas para la aplicación Citrix Workspace para iOS.
  2. Configure los almacenes para StoreFront tal como lo hace para otras aplicaciones de Citrix Virtual Apps and Desktops y Citrix DaaS. No se requiere ninguna configuración especial para los dispositivos móviles. Para obtener detalles, consulte Opciones de acceso de usuarios en la sección de StoreFront de la documentación de productos. Para dispositivos móviles, use alguno de estos métodos:
    - Archivos de aprovisionamiento. Puede dar a los usuarios unos archivos de aprovisionamiento (.cr) que incluyen los datos de conexión con sus almacenes. Después de la instalación, los usuarios abren el archivo en el dispositivo para configurar la aplicación Citrix Workspace para iOS automáticamente. De forma predeterminada, Workspace para sitios web ofrece a los usuarios un archivo de aprovisionamiento para el único almacén para el que esté configurado el sitio en cuestión. También es posible utilizar la consola de administración de Citrix StoreFront con el fin de generar archivos de aprovisionamiento para uno o varios almacenes que se puedan distribuir manualmente a los usuarios.
    - Configuración manual. Es posible informar directamente a los usuarios sobre las direcciones URL de los almacenes o de Citrix Gateway que se necesitan para acceder a sus escritorios y aplicaciones. Para las conexiones a través de Citrix Gateway, los usuarios tam-

bién deben conocer el método de autenticación requerido y la edición de los productos. Después de la instalación, los usuarios deben introducir estos detalles en la aplicación Citrix Workspace, que intenta verificar la conexión y, si la conexión es satisfactoria, solicita a los usuarios que inicien sesión.

- Configuración automática. Toque **Agregar cuenta** en la pantalla de bienvenida e introduzca la URL del servidor StoreFront en el campo de dirección. La configuración de la cuenta tiene lugar inmediatamente cuando se agrega la misma.

### Para configurar Citrix Gateway

Si tiene usuarios que se conectan desde fuera de la red interna, configure la autenticación a través de Citrix Gateway. Por ejemplo, los usuarios que se conectan a través de Internet desde una ubicación remota.

- Cuando se usa StoreFront, la aplicación Citrix Workspace para iOS es compatible con las versiones de Citrix Access Gateway Enterprise Edition a partir de la 9.3, y las versiones de Citrix Gateway hasta la 13.

### Interfaz Web

Para configurar el sitio de la Interfaz Web, los usuarios con dispositivos iPhone e iPad pueden iniciar aplicaciones a través de dicho sitio y el explorador Safari integrado en sus dispositivos móviles. Configure el sitio de la Interfaz Web de la misma forma que configura otras aplicaciones de Citrix Virtual Apps and Desktops. Si no se ha configurado ningún sitio de XenApp y XenDesktop para el dispositivo móvil, la aplicación Citrix Workspace para iOS usa automáticamente el sitio de la Interfaz Web. No se requiere ninguna configuración especial para los dispositivos móviles.

El explorador Safari integrado admite la Interfaz Web 5.x.

### Para iniciar aplicaciones en los dispositivos iOS

En el dispositivo móvil, los usuarios pueden iniciar una sesión en el sitio de la Interfaz Web con sus credenciales normales.

### Aprovisionamiento automático para dispositivos móviles

En StoreFront, utilice las tareas **Exportar archivo de aprovisionamiento multialmacén** y **Exportar archivo de aprovisionamiento** para generar archivos que contengan datos de conexión para los almacenes, incluidas las implementaciones de Citrix Gateway y las balizas configuradas para dichos

almacenes. Ponga estos archivos a disposición de los usuarios para permitirles que configuren la aplicación Citrix Workspace para iOS automáticamente con la información de los almacenes. Los usuarios también pueden obtener los archivos de aprovisionamiento de la aplicación Citrix Workspace para iOS desde los sitios de Workspace para Web.

### **Importante:**

En implementaciones con varios servidores, use solo un servidor a la vez para modificar la configuración del grupo de servidores. Compruebe que la consola de administración de Citrix StoreFront no se está ejecutando en ninguno de los demás servidores de la implementación. Una vez completados, propague los cambios de configuración al grupo de servidores de modo que los demás servidores de la implementación se actualicen.

1. En la pantalla de Inicio o Aplicaciones de Windows, busque el icono de Citrix StoreFront y haga clic en él. Seleccione el nodo Almacenes en el panel izquierdo de la consola de administración de Citrix StoreFront.
2. Para generar un archivo de aprovisionamiento que contenga información de varios almacenes, en el panel Acciones haga clic en Exportar archivo de aprovisionamiento multialmacén y seleccione los almacenes que quiera incluir en el archivo.
3. Haga clic en Exportar y en Guardar para guardar el archivo de aprovisionamiento con la extensión `.cr` en una ubicación adecuada de la red.

## **Información de acceso de usuario**

Debe facilitar a los usuarios la información de cuenta de la aplicación Citrix Workspace para iOS que necesitan para poder acceder a sus aplicaciones, escritorios y datos alojados en servidores. Puede proporcionarles esta información de las siguientes formas:

- Configurar la detección de cuentas basada en direcciones de correo electrónico
- Proporcionar un archivo de aprovisionamiento a los usuarios
- Proporcionar información de cuenta a los usuarios para que la introduzcan manualmente

## **Configurar la detección de cuentas basada en direcciones de correo electrónico**

Puede configurar la aplicación Citrix Workspace para iOS para que use la detección de cuentas basada en correo electrónico. Cuando está configurada, los usuarios introducen su dirección de correo electrónico, en lugar de una dirección URL de servidor, durante la instalación y configuración inicial de la aplicación Citrix Workspace para iOS. La aplicación Citrix Workspace determina el servidor Access Gateway o StoreFront, o bien el dispositivo virtual de Endpoint Management, que está asociado a esa dirección de correo electrónico en función de los registros del servicio (SRV) que contiene el sistema de nombres de dominio (DNS). A continuación, pide a los usuarios que inicien la sesión para acceder a sus aplicaciones, escritorios y datos alojados en servidores.

**Nota:**

La detección de cuentas por correo electrónico no se ofrece si la aplicación Citrix Workspace para iOS se conecta a una implementación de Interfaz Web.

**Agregar el registro de ubicación del servicio DNS (SRV) para habilitar la detección basada en direcciones de correo electrónico**

Durante la configuración inicial, la aplicación Citrix Workspace puede ponerse en contacto con los servidores del sistema de nombres de dominio (DNS) de Active Directory para obtener detalles de los almacenes disponibles para los usuarios. Esto significa que los usuarios no necesitan conocer los detalles de acceso de sus almacenes cuando instalan y configuran la aplicación Citrix Workspace para iOS. En su lugar, introducen sus direcciones de correo electrónico y la aplicación Citrix Workspace contacta con el servidor DNS. Puede recopilar los detalles del dominio de la dirección de correo electrónico.

Para que la aplicación Citrix Workspace pueda localizar los almacenes disponibles en función de las direcciones de correo electrónico de los usuarios:

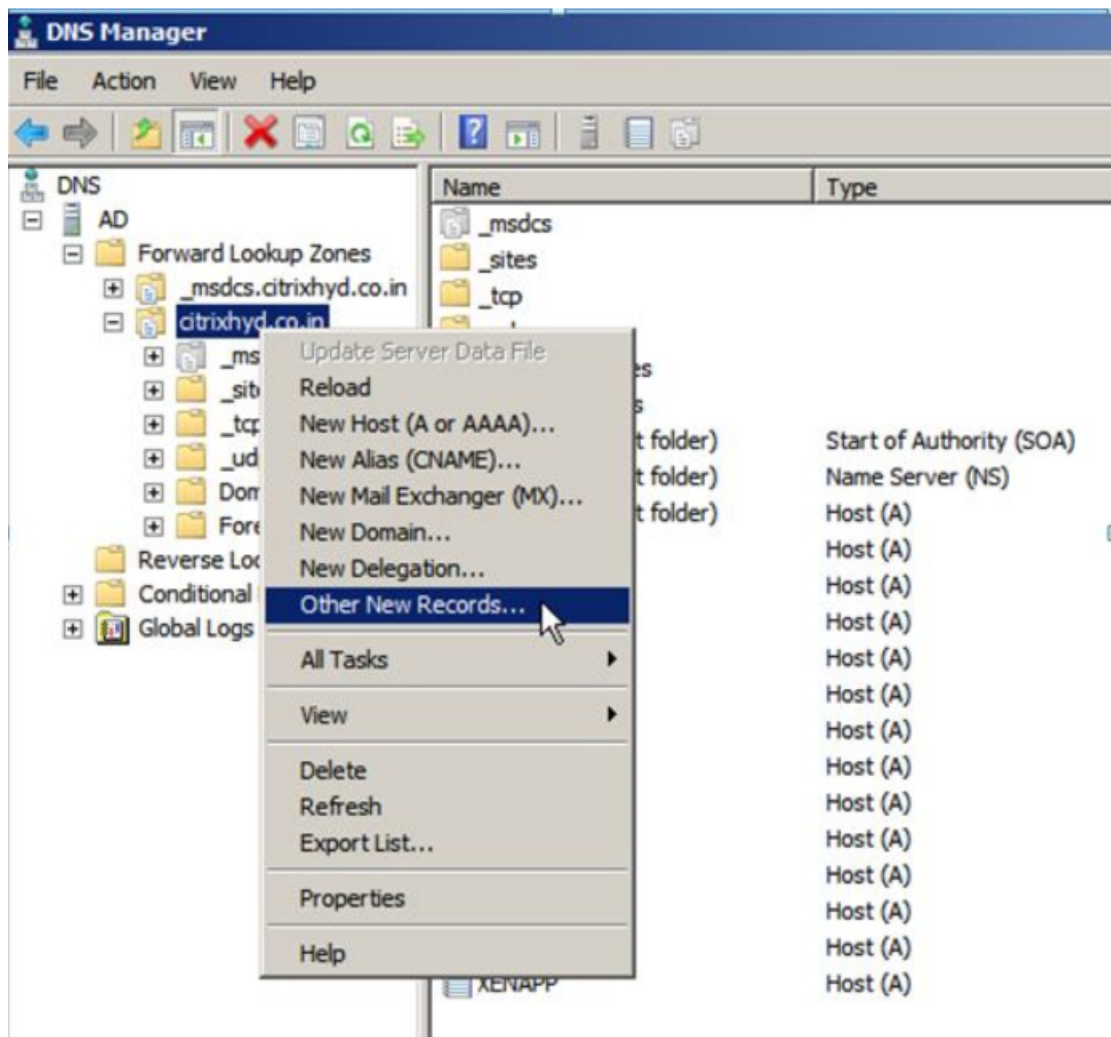
- Configure los registros de recursos del localizador de ubicación del servicio (SRV) para Access Gateway.
- Configure las conexiones de StoreFront o AppController en el servidor DNS.

Para permitir la detección de cuentas basada en direcciones de correo electrónico, es necesario instalar un certificado de servidor válido en el dispositivo Access Gateway y en el servidor de StoreFront o App Controller. También es necesario que la cadena completa al certificado raíz sea válida. Para obtener la mejor experiencia de usuario, instale un certificado con alguna de las opciones siguientes:

- Un asunto
- Una entrada de nombre alternativo de sujeto de *discoverReceiver.domain*.
- Un certificado comodín para el dominio que contenga las cuentas de correo electrónico de los usuarios.

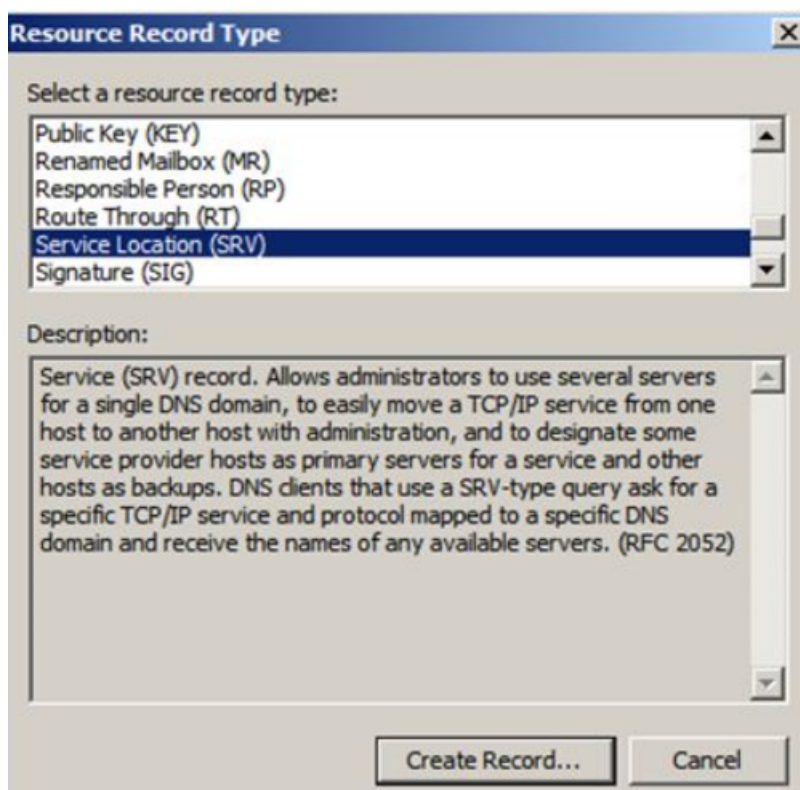
Para permitir a los usuarios configurar la aplicación Citrix Workspace para iOS mediante una dirección de correo electrónico, agregue un registro SRV a la zona DNS de la siguiente manera:

1. Inicie sesión en su servidor DNS.
2. En DNS, haga clic con el botón secundario en su zona de búsqueda directa.
3. Haga clic en **Registros nuevos...**



4. Aparece el cuadro de diálogo **Tipo de registro del recurso**.
5. En **Seleccione el tipo de registro del recurso**, seleccione **Ubicación de servicio (SRV)**.
6. Seleccione **Crear registro**.





7. Aparece el cuadro de diálogo Propiedades.
8. Seleccione la ficha **Ubicación de servicio**.
9. En **Servicio**, introduzca el valor de host\_citrixreceiver.
10. En **Protocolo**, introduzca el valor\_tcp.
11. En **Host que ofrece este servicio**, especifique el nombre de dominio completo (FQDN) y el puerto para su dispositivo Access Gateway (para admitir tanto usuarios locales como usuarios remotos) o el servidor de StoreFront o App Controller (para admitir a los usuarios de la red local únicamente).
12. Haga clic en Aceptar.

**Nota:**

El FQDN de StoreFront debe ser único y diferente del FQDN del servidor virtual de Access Gateway. No se admite el uso de un mismo FQDN para StoreFront y para el servidor virtual de Access Gateway. Citrix Workspace requiere una dirección FQDN de StoreFront única que solo se puede resolver desde dispositivos de usuario conectados a la red interna. De lo contrario, los usuarios de la aplicación Citrix Workspace no pueden utilizar la detección de cuentas basada en direcciones de correo electrónico.

## Entrega de un archivo de aprovisionamiento a los usuarios

Es posible utilizar StoreFront para crear archivos de aprovisionamiento que contengan los detalles de conexión de las cuentas. Usted pone estos archivos a disposición de los usuarios para que puedan configurar la aplicación Citrix Workspace para iOS de forma automática. Después de instalar la aplicación Citrix Workspace para iOS, los usuarios solo tienen que abrir el archivo `.cr` en el dispositivo para configurar la aplicación Citrix Workspace para iOS. Si se configuran sitios de Workspace para Web, los usuarios también pueden obtener los archivos de aprovisionamiento de la aplicación Citrix Workspace para iOS desde esos sitios.

Para obtener más información, consulte la documentación de [StoreFront](#).

## Proporcionar información de cuenta a los usuarios para que la introduzcan manualmente

Si va a entregar a los usuarios los datos de sus cuentas para que luego los introduzcan manualmente, asegúrese de distribuir la siguiente información para permitirles conectar correctamente con sus escritorios alojados en servidores:

- La dirección URL de StoreFront o del sitio de XenApp y XenDesktop que aloja los recursos; por ejemplo, `servername.company.com`.
- Para el acceso mediante Citrix Gateway, proporcione la dirección de Citrix Gateway y el método de autenticación requerido.

Cuando un usuario introduce la información de una cuenta nueva, la aplicación Citrix Workspace intenta verificar la conexión. Si la conexión puede establecerse, la aplicación Citrix Workspace para iOS solicita al usuario que inicie sesión en la cuenta.

## Configurar la aplicación Citrix Workspace

March 28, 2024

En este artículo se enumeran las tareas que le ayudan a configurar la aplicación Citrix Workspace para iOS.

## Administrar marcas de función

Si se produce un problema con la aplicación Citrix Workspace en producción, se puede inhabilitar de manera dinámica la función afectada en la aplicación Citrix Workspace, aunque dicha función ya se haya publicado. Utilizamos marcas de función y un servicio externo denominado LaunchDarkly. No es

necesario que realice ninguna configuración para permitir el tráfico a LaunchDarkly, salvo si tiene un firewall o proxy bloqueando el tráfico saliente. En ese caso, puede habilitar el tráfico a LaunchDarkly a través de direcciones URL o direcciones IP específicas, según sus requisitos de directiva.

Puede habilitar el tráfico y la comunicación en LaunchDarkly de las siguientes formas:

### Permitir el tráfico a las siguientes URL

- [app.launchdarkly.com](https://app.launchdarkly.com)
- [events.launchdarkly.com](https://events.launchdarkly.com)
- [stream.launchdarkly.com](https://stream.launchdarkly.com)
- [clientstream.launchdarkly.com](https://clientstream.launchdarkly.com)
- [Firehose.launchdarkly.com](https://firehose.launchdarkly.com)
- [mobile.launchdarkly.com](https://mobile.launchdarkly.com)

### Incluir direcciones IP en una lista de permitidos

Si necesita incluir las direcciones IP en una lista de permitidos, para obtener una lista de todos los intervalos de direcciones IP actuales, consulte esta [lista de direcciones IP públicas de LaunchDarkly](#). Puede usar esta lista para asegurarse de que las configuraciones de su firewall se actualicen automáticamente de acuerdo con las actualizaciones de la infraestructura. Para obtener detalles sobre el estado actual de los cambios en la infraestructura, consulte el [estado de LaunchDarkly](#).

### Requisitos del sistema para LaunchDarkly

Verifique si las aplicaciones pueden comunicarse con los siguientes servicios si el parámetro de túnel dividido está **desactivado** en Citrix ADC para estos servicios:

- Servicio de LaunchDarkly
- Servicio de escucha de APNs

### Disposición para inhabilitar el servicio de LaunchDarkly:

Puede inhabilitar el servicio de LaunchDarkly tanto en almacenes locales como de la nube.

En la configuración de la nube, puede inhabilitar el servicio LaunchDarkly configurando el atributo `enableLaunchDarkly` en `False`. Puede hacer esto desde la interfaz de usuario de Global App Configuration Service.

```
1 {  
2  
3   "assignedTo": [  
4     "AllUsersNoAuthentication"
```

```
5     ],
6     "category": "Third Party Services",
7     "settings": [
8         {
9
10            "name": "Enable Launch Darkly",
11            "value": "true"
12        }
13    ],
14 ],
15 "userOverride": false
16 }
17
18 <!--NeedCopy-->
```

Para obtener más información, consulte la documentación de [Global App Configuration Service](#).

En la implementación local, haga lo siguiente:

1. Use un editor de texto para abrir el archivo web.config, que normalmente se encuentra en el directorio `C:\inetpub\wwwroot\Citrix\Roaming`.
2. Localice el elemento de la cuenta de usuario en el archivo (Store es el nombre de cuenta de la implementación).

Por ejemplo, `<account id=... name="Store">`

Antes de la etiqueta, vaya a las propiedades de esa cuenta de usuario:

```
1 <properties>
2 <clear/>
3 </properties>
4 <!--NeedCopy-->
```

3. Agregue la etiqueta `enableLaunchDarkly` y el valor como `false`.
4. Agregue la etiqueta `enableLaunchDarkly` y el valor como `false`.

```
<property name="enableLaunchDarkly" value="false"/>
```

**Nota:**

La mayoría de las funciones están detrás de una marca de función controlada por LaunchDarkly. En los entornos en los que está inhabilitada, debe esperar un mínimo de 90 días.

## Tiempo de espera por inactividad para la aplicación Citrix Workspace

Los administradores pueden especificar el tiempo de inactividad permitido. Una vez transcurrido el tiempo de espera indicado, aparece un mensaje de autenticación.

El valor del tiempo de espera por inactividad se puede establecer desde 1 minuto hasta 24 horas. De forma predeterminada, el tiempo de espera por inactividad no está configurado. Los administradores pueden configurar la propiedad `inactivityTimeoutInMinutesMobile` mediante un módulo de PowerShell. Haga clic [aquí](#) para descargar los módulos de PowerShell de la configuración de la aplicación Citrix Workspace.

Cuando haya alcanzado el valor de tiempo de espera especificado, la experiencia del usuario final será la siguiente, según el tipo de autenticación configurado:

- Cuando se agote el tiempo de espera por inactividad, recibirá un mensaje para proporcionar una autenticación biométrica, que le permitirá acceder de nuevo a la aplicación Citrix Workspace.
- Si puede cancelar la solicitud de autenticación biométrica, aparece este mensaje:

**La aplicación Citrix Workspace está bloqueada.**

Debe autenticarse para seguir utilizando la aplicación Workspace.

Si el código de acceso no está configurado en iOS, debe iniciar sesión con las credenciales una vez transcurrido el tiempo de espera por inactividad.

**Nota:**

Esta función solo se aplica a clientes de Workspace (nube).

### Programa para la mejora de la experiencia del usuario (CEIP)

---

Datos recopilados	Descripción	Para qué se usan
Datos de uso y configuración	El programa para la mejora de la experiencia del usuario de Citrix (Customer Experience Improvement Program o CEIP) recopila información de uso y configuración de la aplicación Workspace para iOS y envía esos datos automáticamente a Google Firebase.	Esos datos ayudan a Citrix a mejorar la calidad, la fiabilidad y el rendimiento de la aplicación Workspace.

---

### Información adicional

Citrix gestiona sus datos de acuerdo con las condiciones de su contrato con Citrix. Los datos están protegidos como se especifica en [Citrix Services Security Exhibit](#). Para obtener más información, con-

sulte el [Citrix Trust Center](#).

Citrix utiliza Google Firebase para recopilar determinados datos de la aplicación Citrix Workspace como parte del programa CEIP. Revise cómo gestiona Google los [datos recopilados para Google Firebase](#).

Para dejar de enviar datos de CEIP a Citrix y a Google Firebase:

1. Abra la aplicación Citrix Workspace para iOS.
2. Toque **Inicio > Parámetros**.
3. Vaya a la sección **General**.
4. Inhabilite la opción **Enviar estadísticas de uso**.

**Nota:**

No se recopilan datos de los usuarios de la Unión Europea (UE) ni del Espacio Económico Europeo (EEE) ni de Suiza ni del Reino Unido.

Los elementos específicos de los datos de CEIP que recopila Google Firebase son:

---

Información de sesión y método de inicio de sesión	Almacenes de Citrix y configuración de los almacenes	Tipo de autenticación y configuración de la autenticación	Conexiones ICA
Inicio de sesiones HDX	Sesión de aplicación de almacén	Acción abierta de WebView	Copia de acciones de WebView
Uso compartido de acciones de WebView	Revisión de la aplicación Workspace	Estado de las conexiones, errores de conexión, uso del centro de conexiones	Pantalla externa
Estado de los sockets	Duración de las sesiones	HDX a través de UDP	Hora de los inicios de sesión
Información de dispositivos	Información del modelo del dispositivo	Enviar estadísticas de uso	Idioma de la aplicación y de la aplicación Workspace
Idioma del teclado	Tipo de almacén de Citrix	Combinación de almacenes de Citrix	Tipo de protocolo de los almacenes
Recuento de almacenes	Estado de HDX a través de UDP	Instalaciones de tokens RSA	

---

### Limitaciones conocidas

- En VDA 7.18 y versiones anteriores, la conversión a un Workspace Hub requiere que el escritorio u otro recurso que esté utilizando tenga habilitada la directiva de pantalla completa h.264 y que la directiva de gráficos antiguos esté inhabilitada.

### Sesiones compartidas

Si los usuarios cierran sesión en una cuenta de la aplicación Citrix Workspace, aún pueden cerrar sesión en sesiones remotas o desconectarse de ellas.

- **Desconectar:** Cierra la sesión de la cuenta, pero deja la aplicación o el escritorio de Windows activos en el servidor. El usuario puede iniciar después otro dispositivo, abrir la aplicación Citrix Workspace para iOS y volver a conectarse con el último estado que tenía antes de desconectarse del dispositivo iOS. Esta opción permite a los usuarios reconectarse desde un dispositivo a otro y reanudar el trabajo con las aplicaciones en ejecución.
- **Cerrar sesión:** Cierra la sesión de la cuenta y cierra la aplicación de Windows. También cierra sesión en Citrix Virtual Apps and Desktops y en el servidor de Citrix DaaS. Esta opción permite a los usuarios desconectarse del servidor y cerrar la sesión de la cuenta. Cuando vuelven a iniciar la aplicación Citrix Workspace para iOS, esta se abre en el estado predeterminado.

### Almacenes de la nube

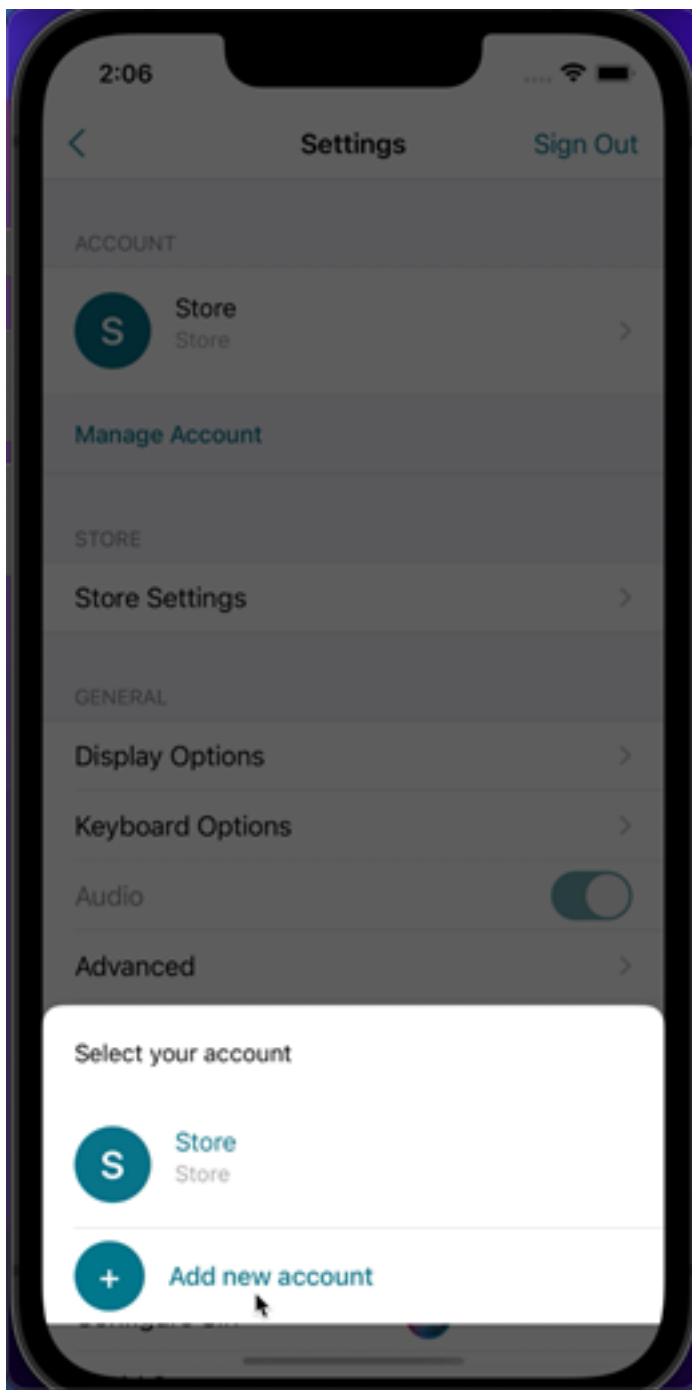
Puede acceder a la web, aplicaciones SaaS y sitios web alojados por su organización independientemente de la ubicación de su acceso. Esta función solo está disponible para clientes de almacenes de la nube.

### Compatibilidad con varios almacenes de la nube

A partir de la versión 24.1.0, puede agregar varias cuentas de almacenamiento en la nube a la aplicación Citrix Workspace para iOS y iPadOS. Ahora, es fácil para los usuarios finales agregar almacenes y cambiar entre ellos. Esta función mejora la experiencia del usuario al acceder a varios almacenes.

Para agregar otra cuenta, siga estos pasos:

1. Vaya a **Parámetros > Administrar cuenta**. Aparecerá un cuadro de diálogo en la parte inferior de la pantalla con una lista de sus cuentas.
2. Toque **Agregar nueva cuenta**.

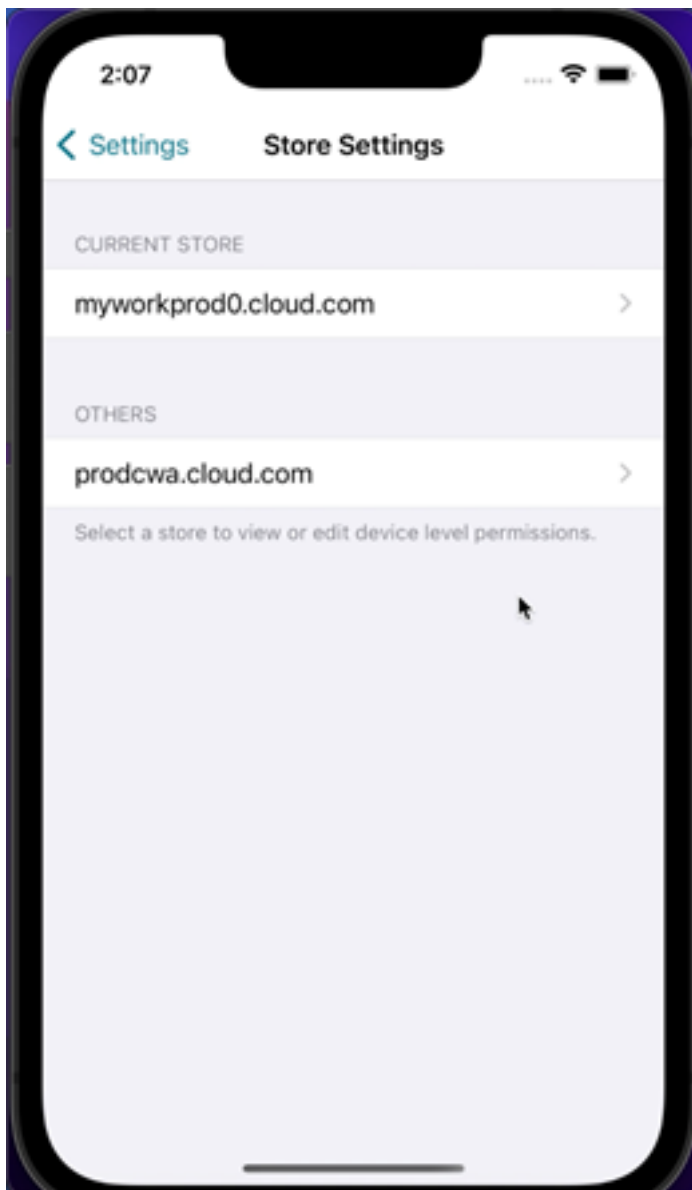


3. Introduzca la dirección URL o de correo electrónico proporcionadas por el administrador de TI. Opcionalmente, para usar una tarjeta inteligente para iniciar sesión, toque **Usar tarjeta inteligente**.
4. Toque **Continuar**. Aparecerá el cuadro de diálogo **Iniciar sesión** con campos para la introducción del nombre de usuario, contraseña, dominio y código de acceso.
5. Introduzca la información correspondiente. Para obtener más información acerca de los cam-



pos, póngase en contacto con su administrador de TI.

6. Toque **Iniciar sesión**. Su nueva cuenta estará configurada ahora.



### **Rellenar automáticamente la URL del almacén**

Al acceder a la aplicación Citrix Workspace para iOS con una nueva personalización de marca, puede elegir rellenar automáticamente la URL del almacén. Esta función reduce las intervenciones manuales y proporciona un acceso rápido a la aplicación. Para obtener más información sobre la personalización de aplicaciones, consulte [App Personalization](#).

## Compatibilidad con la eliminación de varios almacenes a la vez

A partir de la versión 24.2.0, la aplicación Citrix Workspace para iOS permite seleccionar varios almacenes y eliminarlos. Esta función mejora la experiencia del usuario al trabajar con varios almacenes. Esta función está habilitada de manera predeterminada.

Para eliminar varios almacenes a la vez desde la pantalla **Almacenes**, siga estos pasos:

1. En la pantalla **Almacenes**, toque **Seleccionar**.
2. Seleccione los almacenes que quiere eliminar. Para eliminar todos los almacenes, toque **Seleccionar todos**.
3. Toque **Eliminar**.

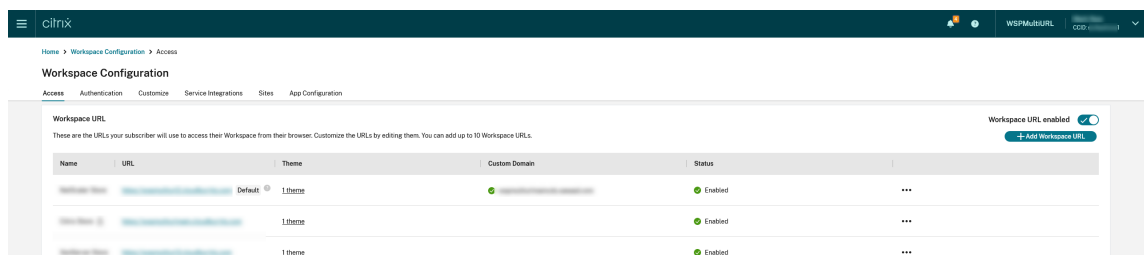
## Función que permite al administrador restringir a los usuarios cambiar el nombre del almacén

Anteriormente, los usuarios podían cambiar el nombre del almacén con la opción **Modificar cuenta**.

A partir de la versión 24.2.0, la aplicación Citrix Workspace para iOS ofrece a los administradores la opción de impedir a los usuarios cambiar el nombre del almacén. Con esta función, los administradores pueden identificar y mantener fácilmente la coherencia de los nombres de los almacenes.

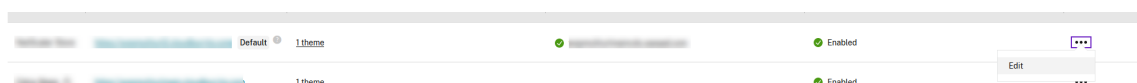
Para permitir a los usuarios finales cambiar el nombre del almacén, siga estos pasos:

1. Inicie sesión en [Citrix Cloud](#) con sus credenciales.
2. Vaya a **Configuración de Workspace > Acceso**. En **URL de Workspace**, puede encontrar una lista de las URL de los almacenes existentes.

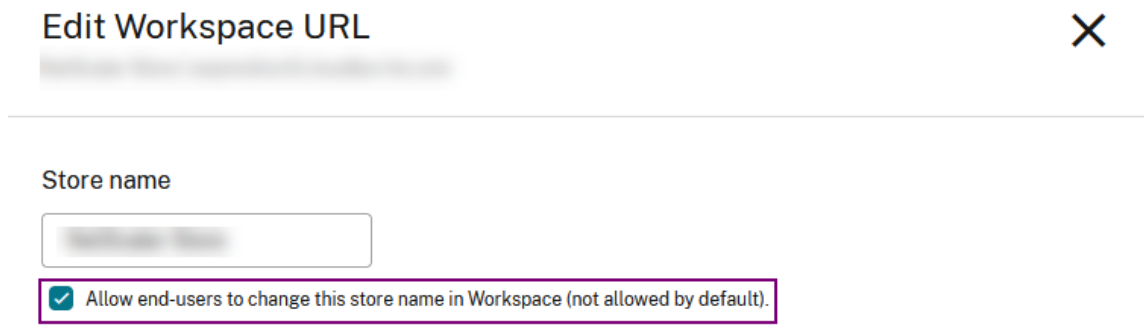


3. Haga clic en el menú de puntos suspensivos del almacén en el que quiere permitir que los usuarios finales cambien el nombre del almacén.

4. Seleccione **Modificar**.



5. En el cuadro de diálogo **Modificar URL de Workspace**, seleccione **Permitir a los usuarios finales cambiar el nombre de este almacén en Workspace (no permitido de forma predeterminada)**.



Store name

Allow end-users to change this store name in Workspace (not allowed by default).

6. Haga clic en **Guardar**.

### Rellenar automáticamente el nombre del almacén

A partir de la versión 24.2.0, la aplicación Citrix Workspace para iOS permite al administrador actualizar los nombres de los almacenes y envía automáticamente los nombres de los almacenes actualizados a los usuarios. Esta función mejora la experiencia del usuario al eliminar la necesidad de intervenir manualmente cuando se actualiza el nombre del almacén.

#### Nota:

Esta función solo tiene efecto si el administrador ha inhabilitado a los usuarios para cambiar el nombre del almacén.

### Mejora de la supervisión de la experiencia de usuario final

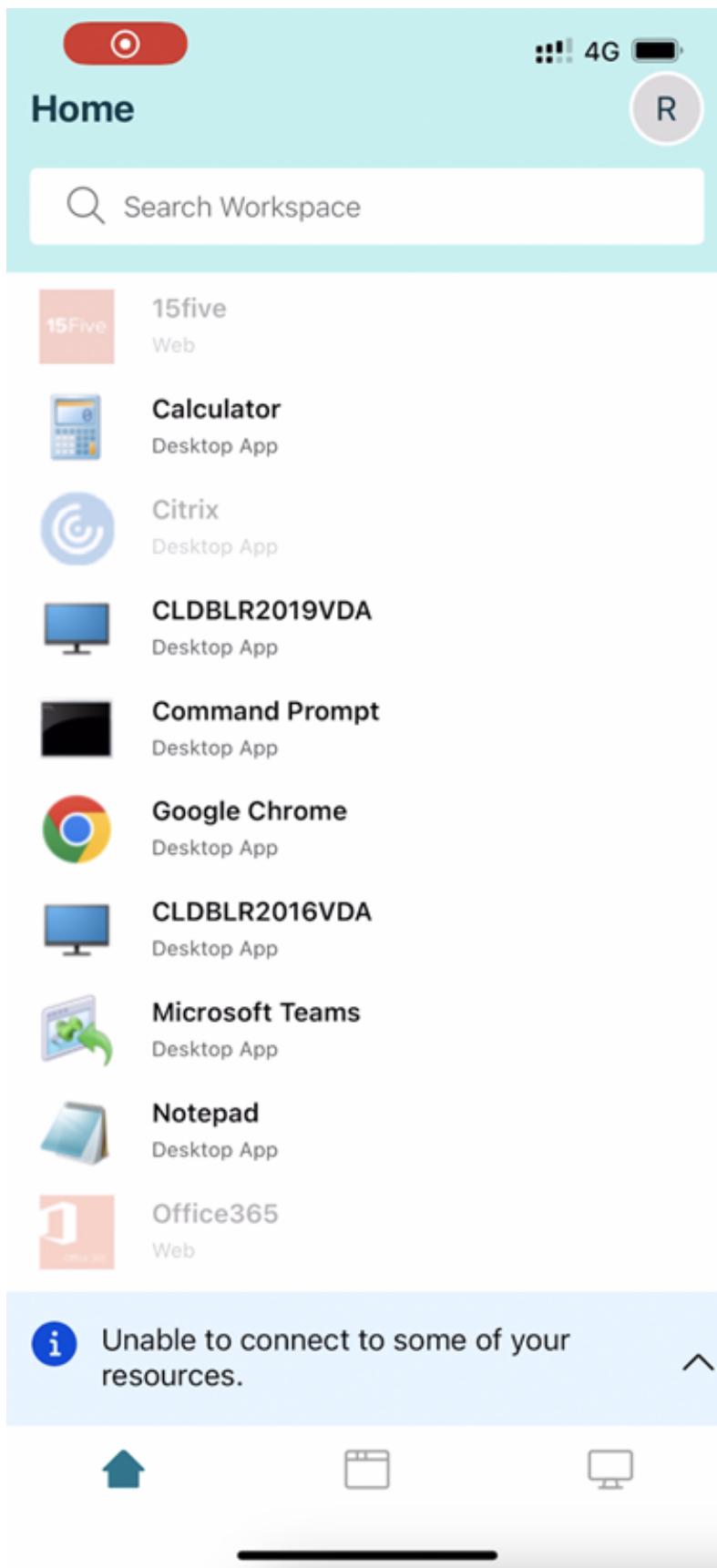
Ahora admitimos las métricas de inicio de clientes de EUEM (End User Experience Monitoring o supervisión de la experiencia del usuario final) EUEM ayuda a recopilar datos de supervisión de la experiencia de sesiones altamente granulares en tiempo real. Envía los datos al panel de mandos de Director para que el administrador pueda supervisar la experiencia de usuario. Los datos se recopilan a través del servicio de supervisión de la experiencia de sesiones (SEMS) presente en el VDA. Los datos de métricas de inicio de clientes disponibles para la supervisión en el panel de mandos incluyen:

- Duración de la descarga de archivos ICA.
- Duración de la creación de sesiones en el cliente. La duración de la creación de sesiones en el cliente representa el tiempo necesario para crear una sesión. Se calcula desde el momento en que se inicia un archivo ICA hasta que se establece la conexión.

- Duración de la búsqueda de sesiones en el cliente. La duración de la búsqueda de sesiones en el cliente representa el tiempo que se tarda en enviar una consulta a cada sesión para alojar la aplicación publicada solicitada. La comprobación se realiza en el cliente para determinar si una sesión existente puede gestionar la solicitud de inicio de la aplicación.
- Grabación en tiempo real de Citrix del tiempo de ida y vuelta de ICA, también conocido como RTT de ICA. El RTT de ICA es el tiempo que transcurre desde que el usuario presiona una tecla hasta que la respuesta se muestra en el dispositivo de punto final.

### **Se ha mejorado la interfaz de usuario para el modo sin conexión de continuidad del servicio**

A partir de la versión 24.1.0, la interfaz de usuario de la aplicación Citrix Workspace para iOS se ha mejorado para hacerla más informativa y moderna, así como para ofrecer una mejor experiencia durante las interrupciones del servicio. La función de búsqueda aproximada también se incluye para el modo sin conexión. Con esta función, puede encontrar resultados de aplicaciones o escritorios con texto parecido y términos de búsqueda mal escritos. Para obtener más información sobre la función de continuidad del servicio, consulte [Continuidad del servicio](#).



## Configurar la aplicación Workspace mediante soluciones de administración unificada de dispositivos de punto final

April 17, 2024

La aplicación Citrix Workspace para iOS admite la configuración administrativa de la aplicación Workspace mediante pares de clave y valor basados en AppConfig con soluciones de administración unificada de dispositivos de punto final (UEM).

### Modo de configuración

Para configurar la URL del almacén de Workspace mediante soluciones de administración unificada de dispositivos de punto final, siga estos pasos:

#### Nota:

A modo de demostración, en este ejemplo se utiliza Microsoft Intune como la solución de UEM. Los pasos que se indican a continuación y la interfaz de usuario que se muestra varían según el proveedor de UEM.

1. Inicie sesión en su proveedor de soluciones de administración unificada de dispositivos de punto final (UEM).
2. Agregue la aplicación Citrix Workspace que quiere que administre su proveedor de UEM. Puede cargar la aplicación mediante el portal de su proveedor de UEM para permitir la administración por parte de su proveedor de UEM. Como alternativa, puede vincular la aplicación en la App Store.
3. Cree una directiva de configuración de aplicaciones para su aplicación.
4. Agregue un par de clave y valor a la lista de propiedades XML y rellene estos valores:

- **clave:** `url`
- **tipo de valor:** `String`
- **valor:** La URL de su almacén (por ejemplo: `prodcwa.cloud.com`)

Settings [Edit](#)

Configuration key	Value type	Configuration value
url	String	prodcwa.cloud.com

## Limitaciones

- Si ya hay un almacén de la nube configurado y el administrador configura un nuevo almacén de la nube, se elimina el almacén de la nube existente. También elimina todos los datos o parámetros asociados del almacén de la nube existente. Recibirá una notificación en Citrix Workspace. A continuación, debe iniciar sesión de nuevo para agregar el nuevo almacén de la nube a Citrix Workspace.
  - Tenga en cuenta que lo anterior solo se aplica a los almacenes de la nube existentes. Si ya hay un almacén local configurado y el administrador configura otro almacén local o de la nube, entonces el nuevo almacén se agrega y no se elimina nada.
- Para aplicar nuevas configuraciones, debe cerrar a la fuerza la aplicación Citrix Workspace y reiniciarla.

## Mejoras en las soluciones de administración unificada de dispositivos de punto final

La aplicación Citrix Workspace para iOS admite un par de configuraciones más mediante pares de clave-valor basados en AppConfig para configurar la aplicación Citrix Workspace. Anteriormente, los administradores podían configurar las URL de los almacenes. Ahora, los administradores pueden restringir a los usuarios finales la posibilidad de modificar las URL de los almacenes y controlar la apariencia de la aplicación.

Configuration key	Value type	Configuration value
url	String	myworkprod0.cloud.com
restrict_user_store_modification	Boolean	true
storeType	Integer	1

Estos son los detalles:

---

Clave de configuración	Tipo de valor	Valor de configuración
<code>url</code>	<code>String</code>	La URL del almacén. Por ejemplo, <code>prodcwa.cloud.com</code>

Clave de configuración	Tipo de valor	Valor de configuración
<code>storeType</code>	Integer	<ul style="list-style-type: none"> <li>(predeterminado) Si se establece en 1, los usuarios pueden ver la carga nativa o predeterminada del almacén. - Si se establece en 2, los usuarios pueden ver el almacén dentro de una interfaz web.</li> </ul>
<code>restrict_user_store_modification</code>	Boolean	<ul style="list-style-type: none"> <li>Si se establece en <b>true</b>, los usuarios no pueden modificar el almacén (agregar/eliminar/modificar). - Si se establece en <b>false</b>, los usuarios pueden modificar el almacén. <b>Nota:</b> Si el indicador se establece en <b>true</b>, se eliminarán todos los almacenes existentes antes de agregar uno configurado por UEM.</li> </ul>

### Función para configurar el nombre del dispositivo a través de UEM

A partir de la versión 24.3.5, la aplicación Citrix Workspace para iOS permite a los administradores asignar e identificar nombres de dispositivos basados en grupos de usuarios a través de Unified Endpoint Management (UEM).

Para configurar el nombre del dispositivo mediante UEM, siga los pasos siguientes:

**Nota:**

A modo de demostración, en este ejemplo se utiliza Microsoft Intune como la solución de UEM. Los pasos que se indican a continuación y la interfaz de usuario que se muestra varían según el proveedor de UEM.

1. Inicie sesión en su proveedor de UEM.
2. Agregue la aplicación Citrix Workspace que quiere que administre su proveedor de UEM. Puede



cargar la aplicación mediante el portal de su proveedor de UEM para permitir la administración por parte de este último. Como alternativa, puede vincular la aplicación en la App Store.

3. Cree una directiva de configuración de aplicaciones para su aplicación.
4. Agregue un par de clave y valor a la lista de propiedades XML y rellene estos valores:
  - clave: deviceName
  - tipo de valor: Cadena
  - valor: Nombre del dispositivo (por ejemplo, MI\_Dispositivo\_iPHONE)

Configuration key	Value type	Configuration value	
url	String	prodcwa.cloud.com	...
deviceName ✓	String ▼	MY_IPHONE_DVICE ✓	...
	Select one ▼		

## Dispositivos periféricos

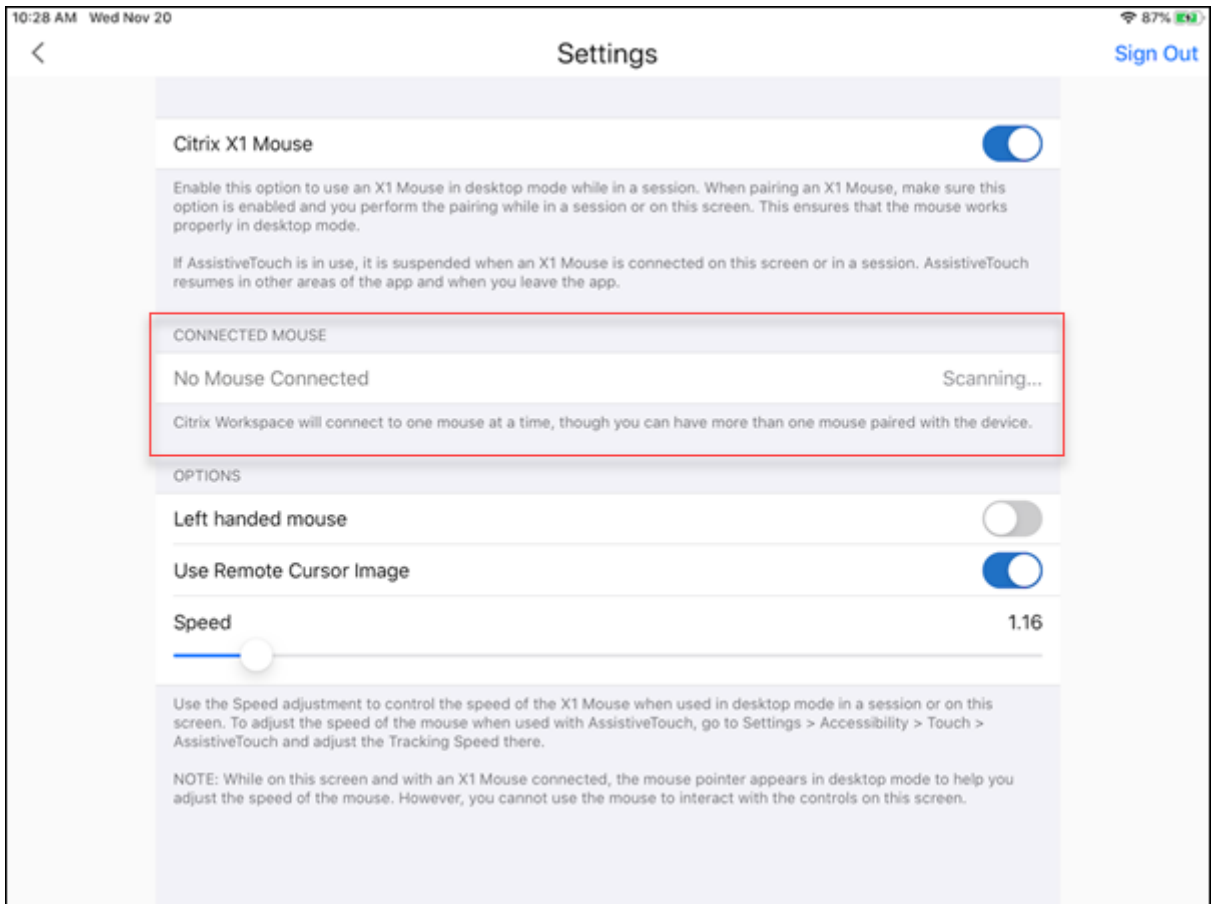
July 1, 2024

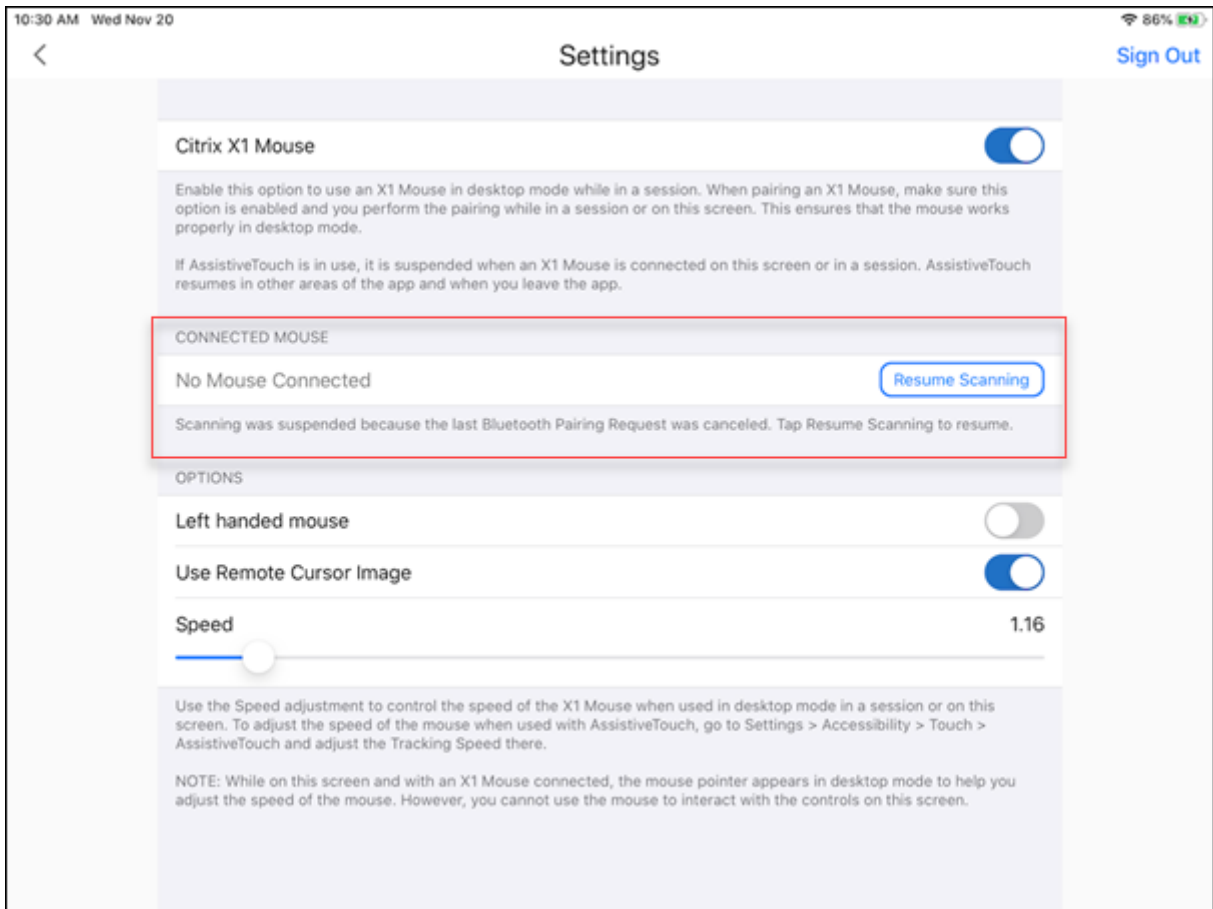
### Citrix X1 Mouse

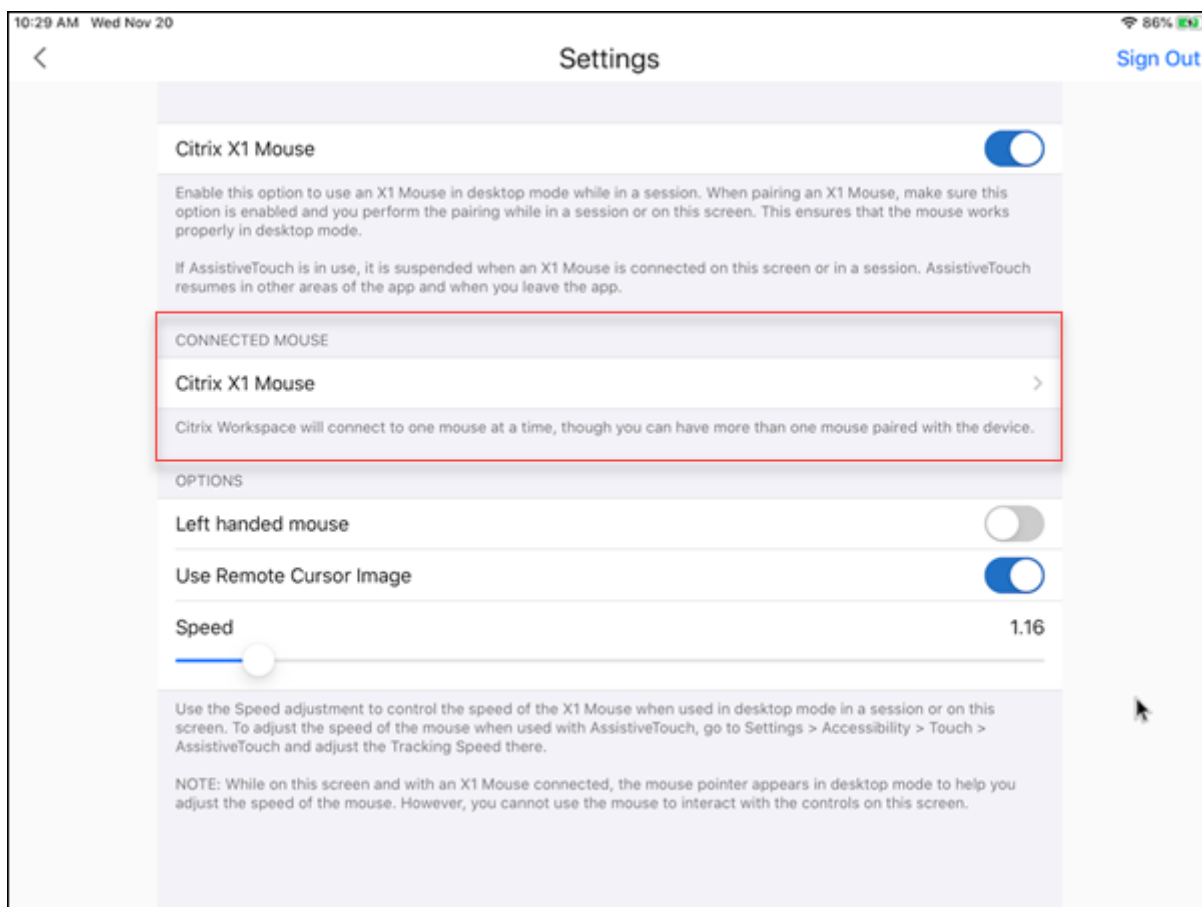
#### Estado de conexión y emparejamiento de dispositivos Citrix X1 Mouse

Esta función le permite tener más control sobre el proceso de emparejamiento de dispositivos Citrix X1 Mouse. En la pantalla **Ajustes**, puede:

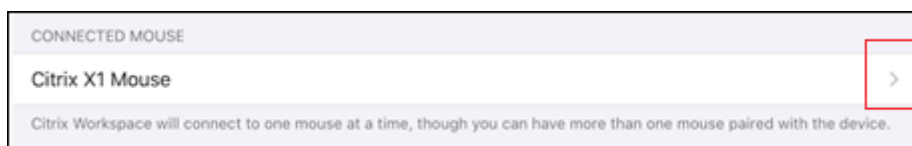
- Emparejar el dispositivo Citrix X1 Mouse. También puede emparejar un dispositivo X1 Mouse cuando se halle en una sesión.
- Ver el estado de la conexión.



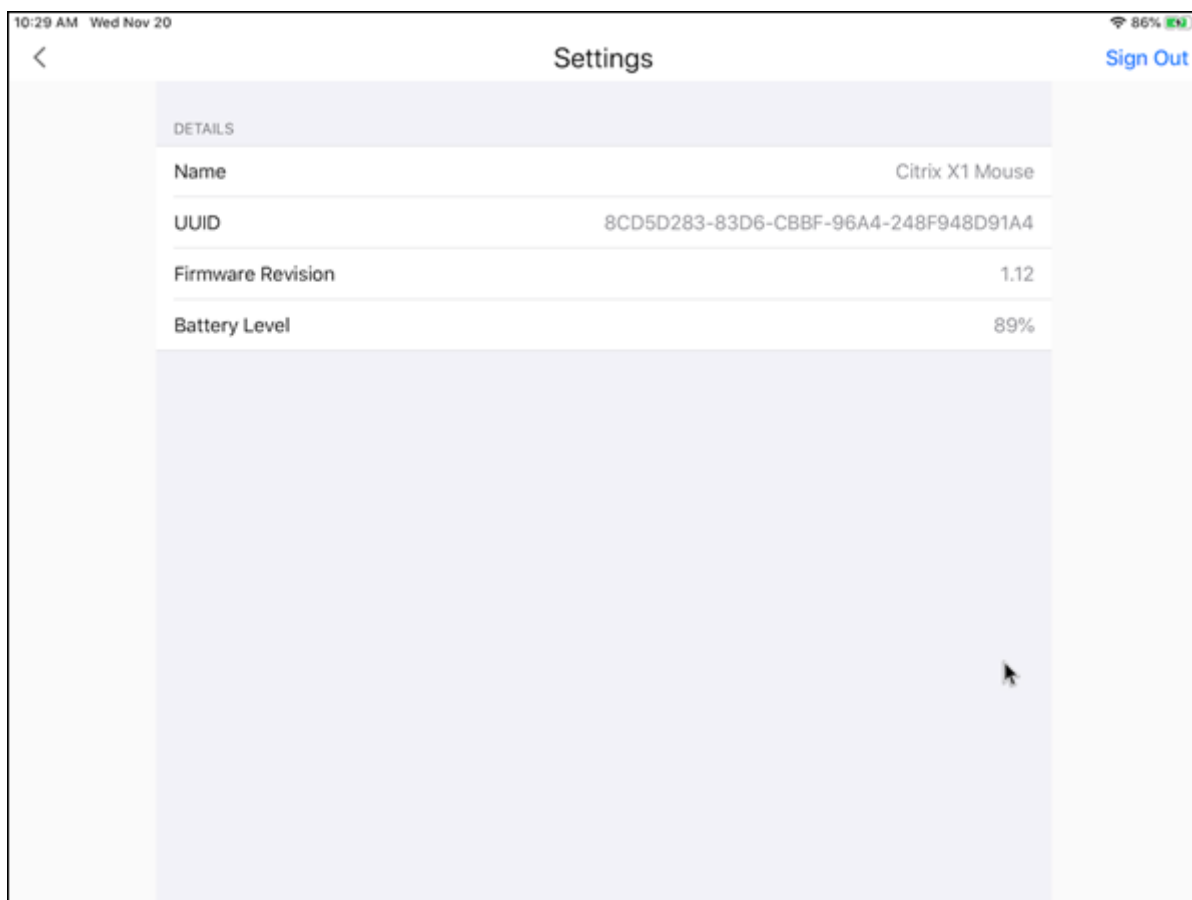




- Consultar las propiedades del dispositivo Citrix X1 Mouse, como, por ejemplo, **Nombre**, **UUID**, **Revisión del firmware** y **Nivel de batería**. Para ello, toque la entrada Citrix X1 Mouse en **MOUSE CONECTADO**.



Propiedades del mouse conectado:



**AssistiveTouch** Con la función AssistiveTouch habilitada en iOS 13 o en versiones posteriores, puede ver el cursor de AssistiveTouch si cambia entre el modo de mouse de escritorio y el modo AssistiveTouch.

**Nota:**

En el modo de mouse de escritorio, aparece el cursor con forma de puntero. En el modo AssistiveTouch, aparece el cursor redondo.

El cursor AssistiveTouch aparece en los siguientes casos:

- Al abandonar una sesión
- Al ir a la pantalla Selector de app de iOS
- Al ir a la pantalla de inicio de iOS u otra aplicación

El modo de escritorio se reanuda cuando vuelve a la aplicación Citrix Workspace y cuando se halla en una sesión.

## Compatibilidad con monitores externos y la barra de herramientas

Puede usar Citrix X1 Mouse para utilizar la barra de herramientas en un monitor externo. Puede mover la muesca de la barra de herramientas horizontalmente mientras esta está cerrada. Al conectar el dispositivo iOS al monitor externo, la aplicación Citrix Workspace detecta automáticamente la resolución de la pantalla de dicho monitor. Puede utilizar el botón **Pantalla** de la barra de herramientas para seleccionar una resolución de pantalla concreta. Puede acceder a la opción **Pantalla** sin tener que agregar una cuenta o iniciar sesión primero.

## Mouse genérico

### Compatibilidad con mouse y paneles táctiles genéricos

Puede utilizar un mouse o un panel táctil para hacer clic con el botón secundario, desplazarse hacia arriba y hacia abajo, y pasar el cursor por sesiones HDX. Las acciones son similares a las de Citrix X1 Mouse. El estilo del cursor del mouse local cambia para que coincida con el del cursor remoto.

#### Notas:

- Esta función está disponible a partir de iPadOS 13.4.
- Esta función no está disponible en iPhones.

**Limitación** Si tiene un monitor externo conectado mientras está en una sesión, el cursor del mouse genérico permanece en el dispositivo nativo debido a una limitación de iOS.

### Compatibilidad con mouse genérico en monitores externos

Puede usar un mouse genérico en monitores externos conectados a un iPad. El mouse genérico se puede usar con dispositivos con iOS 13.4 o una versión posterior.

#### Importante:

Para utilizar un mouse genérico con monitores externos, el modo **Presentación** debe estar desactivado en la aplicación Citrix Workspace, en **Parámetros > Apariencia**.

La barra de herramientas del monitor externo está oculta cuando se usa un mouse genérico. Además, el puntero del mouse se refleja en el monitor externo y aparece simultáneamente tanto en la pantalla del iPad como en el monitor externo.

## Compatibilidad de la prolongación de varios monitores con mouse genérico para iPad

Puede ampliar la sesión de escritorio a un monitor externo cuando conecte su iPad con un mouse genérico. Esta función está disponible a partir de la versión 14.0 de iPadOS.

### Nota:

- Esta función puede estar disponible parcialmente en versiones anteriores. Para utilizar la función completa, actualice la versión a 22.1.0.
- Inhabilite AssistiveTouch en **Ajustes** de iOS > **Accesibilidad** > **Tocar** > **AssistiveTouch** para que la aplicación Citrix Workspace reciba los clics del mouse principal.

## Configurar el modo Prolongar Para habilitar el modo **Prolongar**:

1. Conecte el monitor externo al iPad mediante el cable HDMI y los adaptadores necesarios.

### Nota:

La configuración funciona mejor con un adaptador Lightning a AV digital o un adaptador multipuerto USB-C a AV digital de Apple.

2. Vaya a los **Parámetros** de la aplicación > **Apariencia** y active **Pantalla externa**. Aparecen varios modos de visualización. Los modos Duplicar y Presentación también usan mouse genérico si la versión de iPadOS es 14.0 o una posterior.
3. Seleccione la opción **Prolongar**.

Puede seleccionar uno de estos modos de visualización:

- **Duplicar**: Le permite duplicar la pantalla en el monitor externo conectado al iPad.
- **Presentación**: Le permite cambiar el monitor externo por un panel táctil.
- **Prolongar**: Le permite mostrar diferentes vistas o pantallas en cada pantalla.

### Nota:

- Configure el modo **Prolongar** antes de iniciar y ampliar la sesión de escritorio.
- El modo **Prolongar** no está disponible en iPhones hasta que se anuncie.

## Configurar la disposición de las pantallas Para configurar la disposición de las pantallas:

1. Seleccione el modo **Prolongar** y aparecerá la opción **Disposición de las pantallas**.
2. Recoloque el mosaico de **Pantalla externa** a la izquierda, arriba, a la derecha o abajo de la pantalla del iPad.

### Nota:

Puede ajustar la disposición de la pantalla durante una sesión mediante la barra de herramientas de la sesión > icono de configuración de **pantalla**.

### Nota:

La resolución de la pantalla externa depende de:

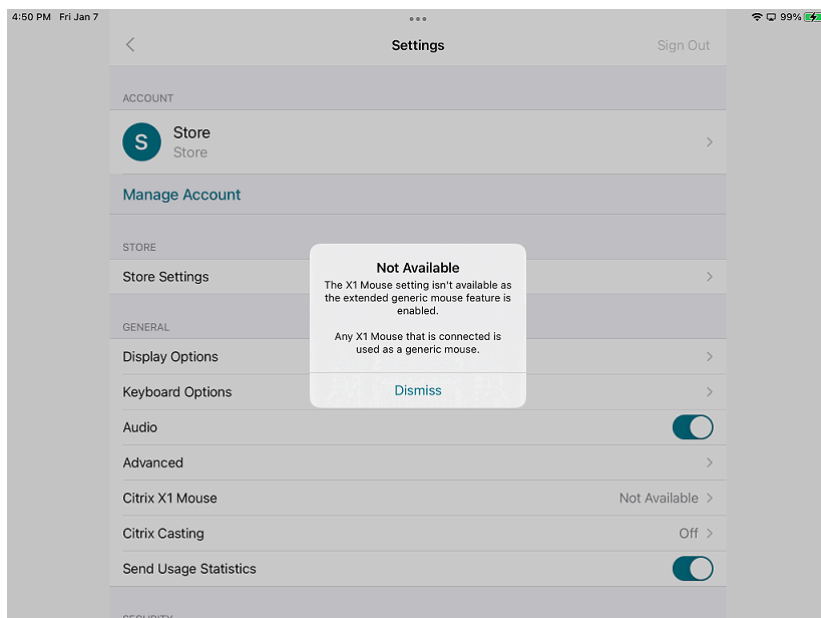
- adaptadores
- iPad
- otro hardware utilizado

## Modo de mouse genérico frente al modo de Citrix X1 Mouse

El modo de mouse genérico tiene prioridad automáticamente ante el modo de Citrix X1 Mouse. Si tiene un dispositivo X1 Mouse conectado, se utiliza como mouse genérico. Por lo tanto, no se puede acceder a la página de parámetros de X1 Mouse cuando la marca de función Mouse genérico está habilitada.

### Nota:

A partir de la versión 14.0 de iPadOS, cualquier dispositivo X1 Mouse que se conecte a un iPad se comporta como un mouse Bluetooth.



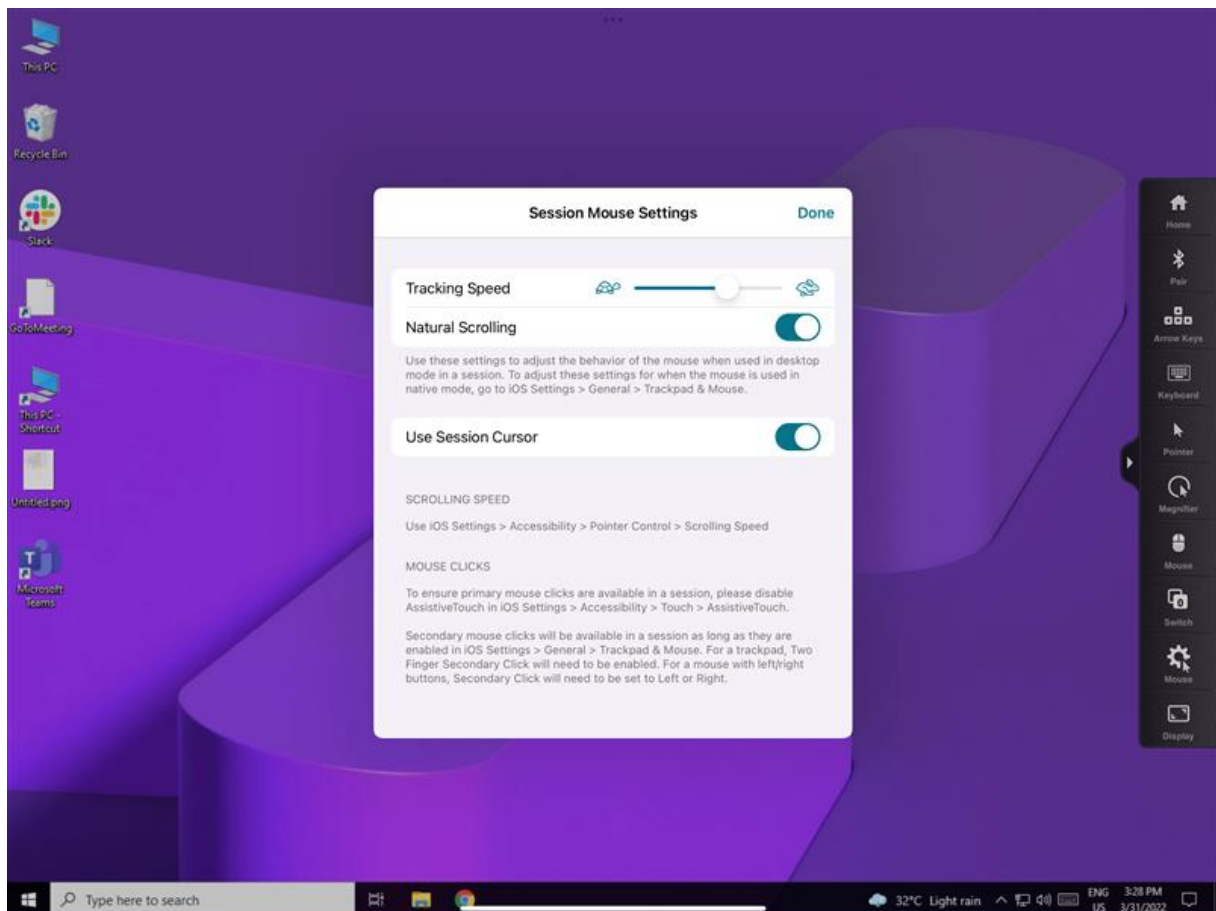


### Icono de mouse genérico

El icono de configuración del **mouse** se agrega a la barra de herramientas de la sesión junto al icono de configuración de **pantalla**. Use los parámetros del **mouse** para ajustar la velocidad de desplazamiento del mouse genérico durante las sesiones. También puede cambiar de mouse mediante la imagen del cursor remoto.

#### Nota:

Puede ajustar la velocidad de desplazamiento del mouse nativo desde los parámetros de iOS.



### Limitaciones de la función

- Para asegurarse de que la aplicación Citrix Workspace reciba los clics del mouse principal, habilite AssistiveTouch en **Ajustes** de iOS > **Accesibilidad** > **Tocar** > **AssistiveTouch**.
- Las opciones de velocidad de desplazamiento y desplazamiento natural de la configuración de iOS no afectan al mouse genérico dentro de la sesión. Sin embargo, la velocidad de desplazamiento se puede controlar desde los **ajustes** de iOS.

Puede acceder a las opciones de velocidad de desplazamiento y desplazamiento natural desde la pantalla de **ajustes del mouse** dentro de la barra de herramientas de la sesión.

- Cuando se usa un iPad en modo dividido y el monitor está conectado, el mouse genérico solo funciona en modo duplicar dentro de una sesión de escritorio.
- Si el cursor nativo está sobre el menú multitarea antes de que la aplicación obtenga el bloqueo del puntero, es decir, antes del inicio de la sesión, no se reciben los eventos del mouse. Como solución temporal, despliegue Centro de notificaciones, mueva el puntero nativo a una ubicación diferente y cierre Centro de notificaciones.
- La redirección de audio falla al conectar un iPad a un monitor externo. El audio se reproduce a través de los altavoces del iPad. [HDX-39159]

### **Problemas conocidos de la función**

- Mientras la sesión está activa, la imagen de escritorio que aparece en un iPad o en un monitor externo se altera cuando cambia:
  - La disposición de las pantallas
  - La resolución
  - La orientación
  - O los modos de pantalla

Como solución temporal, desconecte y vuelva a conectar el monitor. Si el problema persiste, desconéctese y vuelva a iniciar la sesión. [HDX-37038] [HDX-36979] [HDX-36925] [HDX-36924].

- En raras ocasiones, se puede observar un retraso de unos segundos en el audio cuando el vídeo se reproduce en el monitor externo. [HDX-39159]
- En raras ocasiones, la pantalla del VDA se trunca en un iPad y en el monitor externo. Como solución temporal, desconecte y vuelva a conectar el monitor. Si el problema persiste, desconéctese y vuelva a iniciar la sesión. [HDX-37100]
- Al maximizar el vídeo a pantalla completa en el monitor externo, puede que se observen problemas de calidad de vídeo. [HDX-39159]
- En raras ocasiones, al intentar mover las aplicaciones de un iPad al monitor externo dentro de una sesión de escritorio, el proceso falla. Como solución temporal, desconecte y vuelva a conectar el monitor. Si el problema persiste, desconéctese y vuelva a iniciar la sesión. [HDX-36981]
- En raras ocasiones, al conectar un iPad a un monitor externo mediante adaptadores de terceros, los modos de visualización no están disponibles en Opciones de pantalla. [HDX-39713]
- A veces, aparece una línea bajo el puntero del mouse dentro de la sesión del VDA. [RFIOS-9569]

## Teclados

### Sincronización de la distribución de teclado

La sincronización de la distribución del teclado permite a los usuarios cambiar distribuciones de teclado preferidas en el dispositivo cliente. Esta función está inhabilitada de forma predeterminada.

Para habilitar la sincronización de la distribución de teclado, vaya a **Parámetros > Opciones de teclado** y habilite la opción **Sincronización de distribución de teclado**.

#### Nota:

El uso de la opción de distribución de teclado local activa el IME (Input Method Editor) del cliente. Si usted trabaja en japonés, chino o coreano y prefiere usar el editor IME del servidor, inhabilite la opción de distribución de teclado local en **Preferencias > Teclado**.

### Requisitos previos

- Para Linux VDA, habilite la directiva Sincronización de la distribución del teclado del cliente y mejora de IME.
- Para Windows VDA, habilite las directivas Asignación de distribución de teclado Unicode, Sincronización de la distribución del teclado del cliente y Mejora de IME.
- La versión del VDA debe 7.16 o posterior.

### Distribución del teclado con Windows VDA y Linux VDA

Distribución del teclado en iOS	Idioma del teclado	Distribución del teclado en Windows	Distribución de teclado en Linux
Bielorruso (Bielorrusia)	Bielorruso (Bielorrusia)	Teclado bielorruso (Bielorrusia)	by
Búlgaro	Búlgaro	Teclado búlgaro (máquina de escribir)	bg
Chino simplificado	Chino (simplificado, China)	IME de Citrix: chino (simplificado, China)	zh
Chino tradicional	Chino (tradicional, Taiwán)	IME de Citrix: chino (tradicional, Taiwán)	tw
Croata	Croata (Croacia)	Teclado croata	hr
Checo	Checo	Teclado checo	cz
Danés	Danés	Teclado danés	df

Distribución del teclado en iOS	Idioma del teclado	Distribución del teclado en Windows	Distribución de teclado en Linux
Neerlandés	Neerlandés (Países Bajos)	Teclado estadounidense internacional	us
Neerlandés (Bélgica)	Neerlandés	Teclado belga (punto)	be
Inglés (Australia)	Inglés (Australia)	Teclado estadounidense	us
Inglés (Canadá)	Inglés (Canadá)	Teclado estadounidense	us
Inglés (Reino Unido)	Inglés (Reino Unido)	Teclado del Reino Unido	gb
Inglés (EE. UU.)	Inglés (Estados Unidos)	Teclado estadounidense	us
Estonio	Estonio	Teclado estonio	ee
Finlandés	Finlandés	Teclado finés	fi
Francés (Canadá)	Francés (Canadá)	Teclado francés	fr
Francés (Suiza)	Francés (Francia)	Teclado francés suizo	ch
Francés (francés)	Francés (Francia)	Teclado francés	fr
Alemán (Austria)	Alemán (Austria)	Teclado alemán	at
Alemán (Suiza)	Alemán (Suiza)	Teclado alemán suizo	ch
Alemán (Alemania)	Alemán (Alemania)	Teclado alemán	at
Griego	Griego	Teclado griego	gr
Húngaro	Húngaro	Teclado húngaro	hu
Islandés	Islandés	Teclado islandés	is
Irlandés	Irlandés		ie
Italiano	Italiano (Italia)	Teclado italiano	it
Japonés	Japonés	IME de Citrix: japonés	jp
Coreano	Coreano	IME de Citrix: coreano	kr
Letón	Letón	Teclado letón	lv
Noruego	Noruego (Bokmål)	Teclado noruego	no
Polaco	Polaco	Teclado polaco (programadores)	pl

Distribución del teclado en iOS	Idioma del teclado	Distribución del teclado en Windows	Distribución de teclado en Linux
Portugués (Brasil)	Portugués (Brasil)	Teclado portugués (ABNT de Brasil)	br
Portugués (Portugal)	Portugués (Portugal)	Teclado portugués	pt
Rumano	Rumano (Rumanía)	Teclado rumano (antiguo)	ro
Ruso (Rusia)	Ruso	Teclado ruso	ru
Eslovaco	Eslovaco	Teclado eslovaco	sk
Esloveno	Esloveno	Teclado esloveno	si
Español (México)	Español (México)	Teclado latinoamericano	latam
Español (España)	Español (España)	Teclado español	es
Sueco (Suecia)	Sueco (Suecia)	Teclado sueco	se
Turco	Turco	Teclado F turco	tr
Ucraniano	Ucraniano	Teclado ucraniano	ua

### Disponibilidad de teclas especiales

Puede usar estas teclas individuales en un teclado externo a partir de iOS 13.4:

- RePág
- AvPág
- Inicio
- Fin
- F1
- F2
- F3
- F4
- F5
- F6
- F7
- F8
- F9
- F10
- F11

- F12

### **Disponibilidad de combinaciones de teclas especiales**

En esta versión se admiten las siguientes combinaciones de teclas en teclados externos de iOS:

- Windows + R
- Windows + D
- Windows + E
- Windows + L
- Windows + M
- Windows + S
- Windows + CTRL + S
- Windows + T
- Windows + U
- Windows + Número
- Windows + Flecha arriba
- Windows + Flecha abajo
- Windows + Flecha izquierda
- Windows + Flecha derecha
- Windows + X
- Windows + K
- CTRL + ESC

### **Mejoras en el teclado extendido**

A partir de la versión 23.5.0, se ha mejorado la funcionalidad de teclado extendido para ofrecer una mejor experiencia de usuario. Las mejoras son las siguientes:

- Anclaje o desanclaje de la interfaz de usuario de la barra de herramientas extendida.
- Rotación de la barra de herramientas extendida en sincronía con la rotación de la pantalla.
- Compatibilidad con la tecla con el logotipo de Windows y los accesos directos que son combinación de 3 teclas.
- Mejora de la experiencia cuando se utilizan varios monitores.
- Apertura y contracción automáticas de la interfaz de usuario de la barra de herramientas extendida.
- Mejora de la experiencia en el modo del organizador visual (en iPad con chip M1).

## Interfaz de usuario del editor IME

En general, el editor IME proporciona componentes de interfaz de usuario como la ventana de candidatos y la ventana de redacción. La ventana de redacción contiene los caracteres redactados y los elementos de la interfaz de usuario de redacción; por ejemplo, el subrayado y el color de fondo. La ventana de candidatos muestra la lista de candidatos.



La ventana de redacción le permite distinguir entre los caracteres confirmados y los caracteres que se están escribiendo. La ventana de redacción y la ventana de candidatos se mueven con el cursor de entrada de texto.

Como resultado, la función proporciona:

- Una mejora a la hora de escribir caracteres en la ubicación del cursor en la ventana de redacción.
- Una mejor visualización de la ventana de redacción y de la ventana de candidatos.

Puede usar esta función en las sesiones alojadas en los VDA de Windows y está disponible tanto para teclados virtuales como para teclados físicos externos.

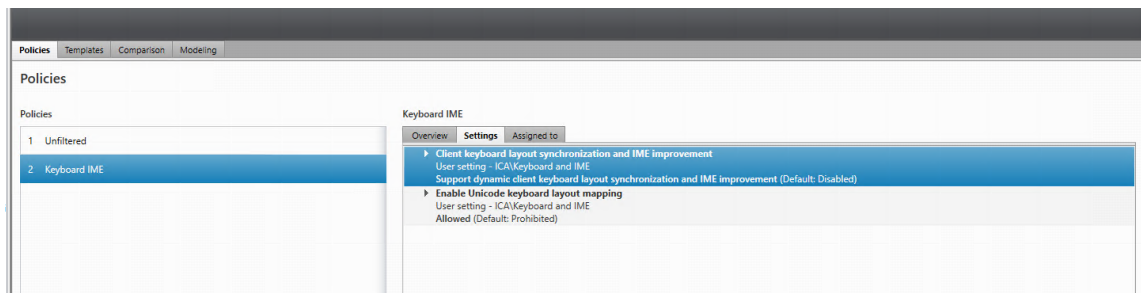
## IME de cliente genérico para idiomas de Asia Oriental

La función del editor de métodos de entrada (IME) de cliente genérico mejora la experiencia para escribir y ver caracteres en chino, japonés y coreano (CJK) en dispositivos iOS. Esta función le permite

componer caracteres CJK en la posición del cursor cuando está en una sesión con sus IME cliente. La función está disponible para los entornos de Windows VDA. Se recomienda utilizar el IME del cliente en lugar del IME del VDA para que la experiencia de usuario sea óptima.

### Requisitos previos

- Habilite la sincronización de la distribución del teclado del cliente y mejora del IME, y habilite la asignación de la distribución del teclado Unicode en el VDA de Windows a través de la directiva de grupo.



Para obtener más información, consulte el artículo de Knowledge Center [CTX312404](#).

También puede habilitar las opciones mediante estos Registros en el VDA de Windows:

- ```
1 - HKLM\Software\Citrix\ICA\IcaIme\DisableKeyboardSync value = DWORD 0
2 - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxKlMap\EnableKlMap value =
  DWORD 1
3 - HKEY_LOCAL_MACHINE\SOFTWARE\Citrix\CtxKlMap\DisableWindowHook value
  = DWORD 1
```

- Habilite **Parámetros > Opciones de teclado > opción Sincronización de distribución de teclado** en la aplicación Citrix Workspace.

### Compatibilidad con el modo de entrada de texto Scancode

A partir de la versión 24.1.0, puede seleccionar **Scancode** como modo de entrada del teclado mientras usa un teclado físico externo. Esta función resulta útil cuando usa dispositivos iOS con un teclado estándar externo para PC con Windows. Con **Scancode**, puede usar la distribución del teclado del VDA en lugar del teclado virtual de iOS. De esta forma, puede seguir completamente el estilo de entrada del teclado externo de Windows en lugar de iOS. Eso resulta muy útil cuando se escribe en idiomas de Asia oriental, ya que mejora significativamente la experiencia general del usuario. Es posible que el usuario final use la distribución del teclado del servidor en lugar de usar la del cliente. Para obtener más información, consulte la sección [Caso de uso](#) de este artículo.

Para usar la función **Scancode**, siga estos pasos:

1. Abra la aplicación Citrix Workspace para iOS y vaya a **Parámetros > Opciones de teclado**.



2. Toque **Modo de entrada del teclado externo**.

3. Seleccione una de estas opciones:

- **Scancode:** Envía la posición de la tecla del teclado del lado del cliente al VDA y el VDA genera el carácter correspondiente. Aplica la distribución del teclado del lado del servidor.
- **Unicode:** Envía la tecla del teclado del lado del cliente al VDA, y el VDA genera el mismo carácter en el VDA. Aplica la distribución del teclado del lado del cliente.

De forma predeterminada, **Unicode** está seleccionado como modo de entrada tanto para el teclado de software o táctil como para el teclado externo.

4. Toque **Scancode**.

Durante una sesión, puede cambiar la distribución y entrada del teclado remoto, del servidor o del VDA por la distribución del teclado remoto, del servidor o del VDA.

**Caso de uso** Por ejemplo, imagine una situación en la que usa una distribución de teclado internacional de EE. UU. que está conectado a su dispositivo iOS.

Si elige **Scancode** y pulsa la tecla situada junto a Bloq Mayús en el teclado externo, se envía al VDA el **código de escaneo 1E**. Entonces el VDA usa **1E** para mostrar el carácter **a**.

Si elige **Unicode** y pulsa la tecla situada junto a Bloq Mayús en el teclado externo, se envía al VDA el carácter **a**. Por lo tanto, aunque el VDA utilice otra distribución de teclado con un carácter diferente en la misma posición, en la pantalla se mostrará el carácter **a**.

**Nota:**

**Unicode** es el modo preferido para escribir cuando se utiliza un teclado táctil en dispositivos móviles. Esto se debe a que las teclas de un teclado táctil no suelen generar un código de escaneo.

### Mejoras en la compatibilidad con accesos directos de teclados externos

La aplicación Citrix Workspace para iOS ahora le permite usar más accesos directos de teclados externos en una sesión de escritorio o aplicación remotos. Las siguientes son mejoras importantes realizadas en los accesos directos de teclados externos:

- Compatibilidad con teclas específicas del teclado Windows, como **Insert**, **Supr** y el teclado numérico.
- Si mantiene presionada una tecla y no la suelta, la aplicación o el escritorio remoto responden correctamente.
- Compatibilidad con accesos directos de más de tres teclas.

Además, ahora puede configurar la tecla específica para **Alt** mediante las siguientes opciones de **Parámetros > Opciones de teclado > Asignar tecla específica para Alt**:

- **Opción o Alt (izquierda)**: envía **Alt** mediante **Opción (izquierda) o Alt (izquierda)**.
- **Comando o Windows (izquierda)**: envía **Alt** mediante las teclas **Comando (izquierda) o Windows (izquierda)**.
- **Opción o Alt (izquierda y derecha)**: envía **Alt** mediante la tecla **Opción o Alt (izquierda y derecha)**.

La opción **Asignar tecla específica para Alt** ayuda a evitar conflictos entre la tecla **Opción** de macOS y la tecla **Alt** de Windows.

**Limitaciones** Actualmente, no se admiten los siguientes accesos directos del sistema iOS:

- **Comando (Windows)-H**: va a la pantalla de inicio.
- **Comando (Windows)-Barra espaciadora**: muestra u oculta el campo de búsqueda.
- **Comando (Windows)-Tabulador**: cambia a la aplicación utilizada más recientemente de entre las aplicaciones abiertas.
- **Comando (Windows)-Mayús-3**: toma una captura de pantalla.
- **Comando (Windows)-Mayús-4**: toma una captura de pantalla y abre inmediatamente Marcación para verla o modificarla.
- **Comando (Windows)-Opción (Alt)-D**: muestra u oculta el Dock.
- **Comando (Windows)-Ctrl-Q**: bloquea el dispositivo.
- **AltGr** no está disponible en el teclado para Europa. Si quiere introducir caracteres especiales con **AltGr**, use en su lugar los siguientes accesos directos:
  - Acceso directo **Opción+\*** en macOS o
  - **Alt + método abreviado de teclado numérico** en el sistema operativo Windows.

## Acceso al micrófono y a la cámara

Ya puede acceder al micrófono y a la cámara para conferencias de audio y vídeo en sesiones de VDA. La aplicación Citrix Workspace requiere su permiso para acceder al micrófono o a la cámara, que se puede proporcionar desde **Parámetros**, en el dispositivo, donde se habilitan la cámara o el micrófono.

Además, se ha incluido el acceso al micrófono y a la cámara por almacén como parte de la función de seguridad de confianza en clientes selectivos para permitir que la aplicación Citrix Workspace confíe en el acceso desde una sesión de VDA.

La aplicación Citrix Workspace requiere el permiso del usuario para acceder al micrófono o a la cámara.

Para configurar los niveles de acceso, vaya a **Parámetros > Parámetros del almacén**. En el menú **Parámetros del almacén**, haga clic en un almacén para habilitar el acceso necesario al micrófono o a la cámara. La configuración seleccionada para el micrófono o el acceso al micrófono se aplica por almacén.

### **Compatibilidad con cámara trasera**

Ahora, la aplicación Citrix Workspace para iOS le permite cambiar de la cámara frontal a la trasera y viceversa dentro de la sesión de VDA.

Aparece un botón flotante al invocar la cámara. Toque una vez en el botón flotante para cambiar entre la cámara frontal y la trasera.

También puede mover el botón flotante libremente por la pantalla y colocarlo donde quiera.

### **Problemas conocidos:**

El botón flotante queda tapado parcial o totalmente cuando la función de proyección o la función de escaneo de documentos se habilitan.

## **Gráficos y pantalla**

### **Rendimiento gráfico mejorado**

A partir de la versión 24.1.0, la aplicación Citrix Workspace para iOS admite la codificación o descodificación de vídeo H.264 acelerada por hardware. Ahora, el motor multimedia de Citrix HDX usa el marco Video Toolbox de Apple para la codificación y la descodificación. Este marco comprime y descomprime vídeo más rápido y en tiempo real. Esta mejora reduce la carga de la CPU durante el uso multimedia.

### **Asignación de unidades del cliente (CDM)**

Puede seleccionar un acceso de almacenamiento de dispositivo específico para cada almacén configurado. El acceso al almacenamiento de dispositivos tiene las siguientes opciones.

- Sin acceso
- Acceso de solo lectura
- Acceso de lectura y escritura
- Preguntar cada vez

Si selecciona **Preguntar cada vez**, aparece un mensaje en el que se le pide que seleccione el tipo de acceso al almacenamiento del dispositivos en cada inicio. De forma predeterminada, está seleccionada la opción **Sin acceso**.

**Nota:**

Esta función solo se aplica en los inicios directos de ICA y en los almacenes configurados de Citrix Gateway. No es compatible con almacenes que no tienen una configuración SSL de extremo a extremo.

Los parámetros de **Almacenamiento de dispositivos** están disponibles en una nueva sección de configuración denominada **Parámetros del almacén**. Para ver **Almacenamiento de dispositivos**, vaya a **Parámetros > Parámetros del almacén**.

## Citrix Ready Workspace Hub

Citrix Ready Workspace Hub combina entornos digitales y físicos para entregar aplicaciones y datos dentro de un espacio inteligente y seguro. El sistema completo conecta dispositivos (o cosas), como aplicaciones móviles y sensores, para crear un entorno inteligente que responda adecuadamente.

Citrix Ready Workspace Hub se ha construido sobre la plataforma Raspberry Pi 3. El dispositivo que ejecuta la aplicación Citrix Workspace se conecta a Citrix Ready Workspace Hub y transmite las aplicaciones o los escritorios hacia una pantalla más grande.

Para obtener más información sobre Citrix Ready Workspace Hub, consulte la documentación de [Citrix Ready Workspace Hub](#).

Por motivos de seguridad, Citrix Ready Workspace Hub admite conexiones SSL con dispositivos móviles. Establezca un nombre de dominio completo (FQDN) de manera manual o automática para identificar de forma única cada dispositivo. Para obtener más información, consulte [Conexión de seguridad](#) en la documentación de Citrix Ready Workspace Hub.

Citrix Ready Workspace Hub se habilita en la aplicación Citrix Workspace cuando se cumplen todos los requisitos de sistema siguientes:

- Aplicación Citrix Workspace 1810.1 para iOS o versiones posteriores
- Bluetooth habilitado
- El dispositivo móvil y Workspace Hub deben utilizar la misma red Wi-Fi

## Configurar Citrix Ready Workspace Hub

Para activar las funciones del concentrador de Citrix Ready Workspace Hub, vaya a **Parámetros** y toque **Citrix Casting** para habilitar la función en su dispositivo. Para obtener más información, consulte la documentación para dispositivos [iOS](#).

La aplicación Citrix Workspace integra un nuevo procedimiento para agregar o quitar un Workspace Hub de la lista de confianza en dispositivos iOS. Para obtener más información, consulte [Conexión de seguridad](#).

## **Función disponible para escáner de documentos**

A partir de la versión 24.5.0, la aplicación Citrix Workspace para iOS admite la función de escáner de documentos. Con esta función, ahora puede escanear y guardar varios documentos, todo ello dentro de la sesión de escritorio. Esta función está habilitada de manera predeterminada.

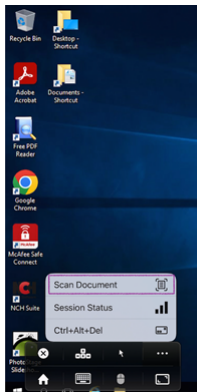
### **Requisitos previos**

- La asignación de unidades del cliente (CDM) debe estar habilitada para el almacén.
- La función del escáner de documentos requiere acceso de lectura y escritura en el dispositivo. Para habilitar el acceso, siga estos pasos:

1. Desde su perfil, toque **Parámetros de aplicación > Parámetros de almacén**.
2. Toque su almacén actual.
3. Toque **Almacenamiento del dispositivo** y después seleccione **Acceso total**.

Para digitalizar documentos con el escáner de documentos, siga estos pasos:

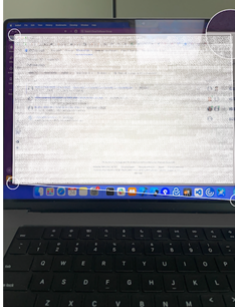
1. En la barra de herramientas de la sesión, toque el menú de tres puntos y seleccione **Escanear documento**. Se abre la aplicación de la cámara.



2. Toque el botón del obturador para capturar la foto. Si decide volver a capturar, toque **Tomar de nuevo**.



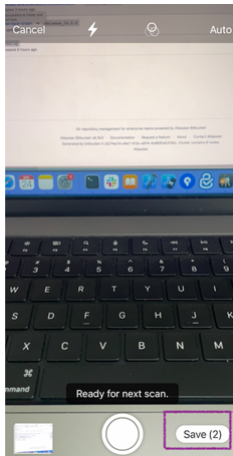
3. Opcional: recorte el documento escaneado. Después de recortarlo al tamaño que quiera, toque **Mantener escaneado**. La aplicación de la cámara se abre de nuevo para que pueda capturar más imágenes.



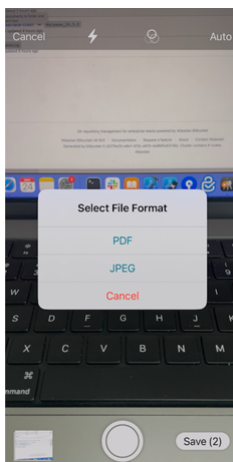
Retake

Keep Scan

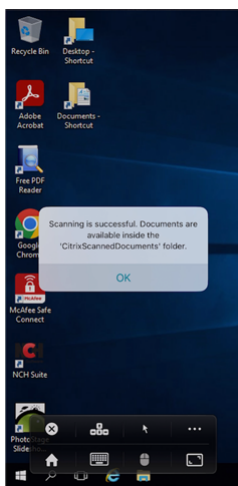
4. Tras capturar las imágenes necesarias, toque **Guardar**.



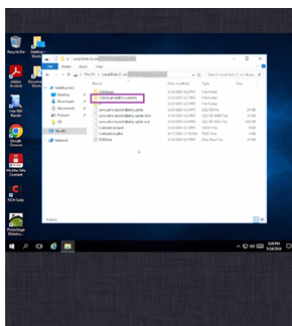
5. Para guardar el documento escaneado en el formato que quiera, seleccione la opción de formato de archivo.



6. Toque **Aceptar**.



Se puede acceder a todos los documentos escaneados dentro de la carpeta **CitrixScannedDocuments** del almacenamiento local del dispositivo. También puede acceder a los **CitrixScannedDocuments** en el administrador de archivos de sesión.

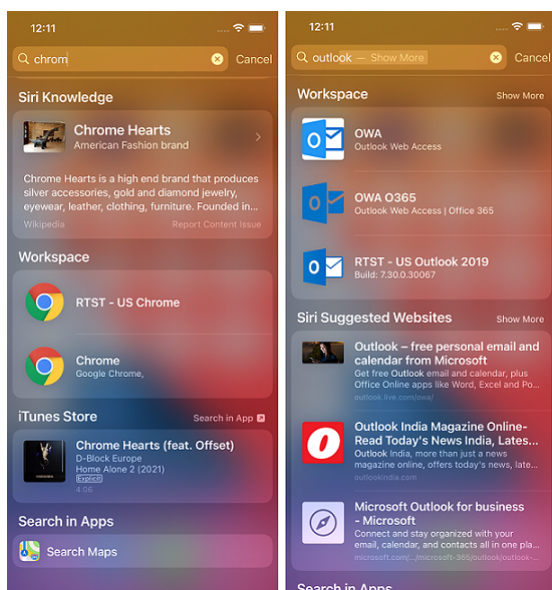


## Experiencia de usuario

March 28, 2024

### Mejora en la búsqueda de Spotlight

El icono de la aplicación coincide con la búsqueda de la aplicación correspondiente. Antes se mostraba el icono de la aplicación Citrix Workspace para todas las búsquedas.



### Acceso a aplicaciones recientes mediante gestos de 3D Touch

Puede acceder a una lista de aplicaciones iniciadas recientemente como acceso rápido cuando utiliza el gesto de 3D Touch (toque largo) en el icono de la **aplicación Citrix Workspace**.

### Indicador de estado de la batería

Ahora, el estado de la batería del dispositivo aparece en el área de notificaciones dentro de la sesión del escritorio virtual.

Esta función solo está disponible en VDA 7.18 y versiones posteriores.

#### **Nota:**

En sesiones en VDA con Microsoft Windows 10, es posible que el indicador de estado de la batería tarde entre 1 y 2 minutos en aparecer.

### Funcionalidad de pulsación larga para acceder a recursos

Ahora puede pulsar de forma prolongada el icono de la aplicación Citrix Workspace y acceder al último recurso que inició. Ahora puede salir de la aplicación Citrix Workspace y acceder al último recurso que inició.

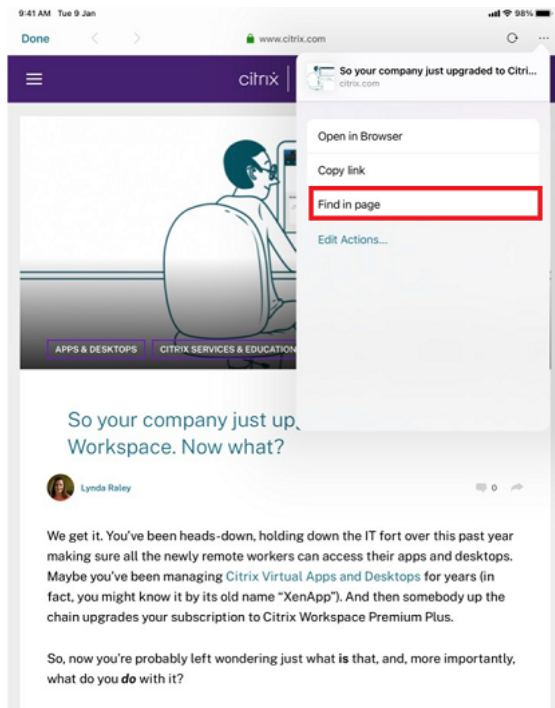


## Mejora en Buscar en la página

La mejora en Buscar en la página le permite buscar palabras y frases. Esta mejora de usabilidad está disponible en sus aplicaciones web y de software como servicio (SaaS).

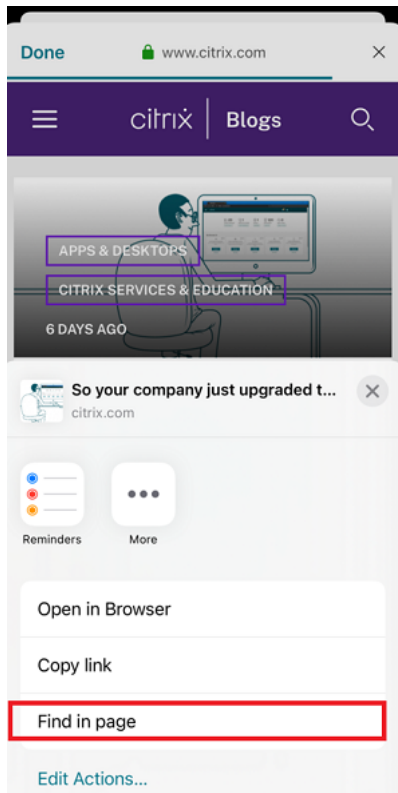
Para realizar una búsqueda:

1. En el iPad, toque el botón de puntos suspensivos (...) de la esquina superior derecha y seleccione **Buscar en la página**.

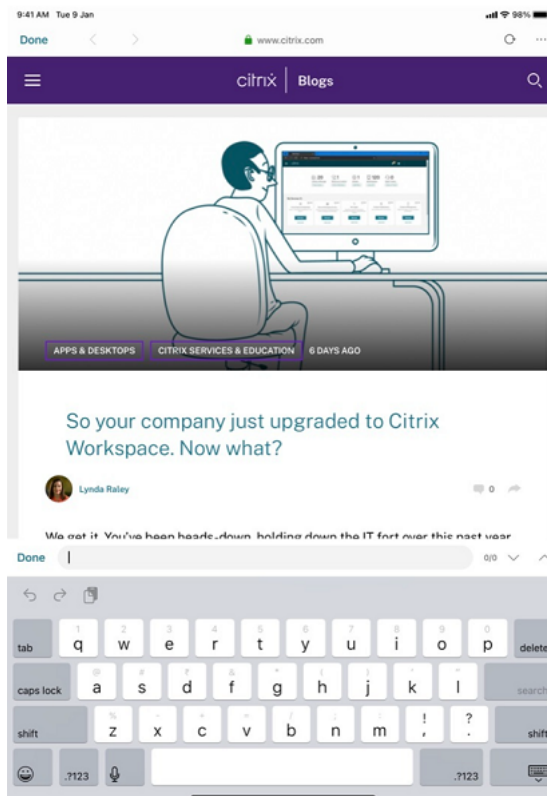


En el iPhone, toque el botón de puntos suspensivos (...) de la esquina inferior derecha y seleccione **Buscar en la página**.

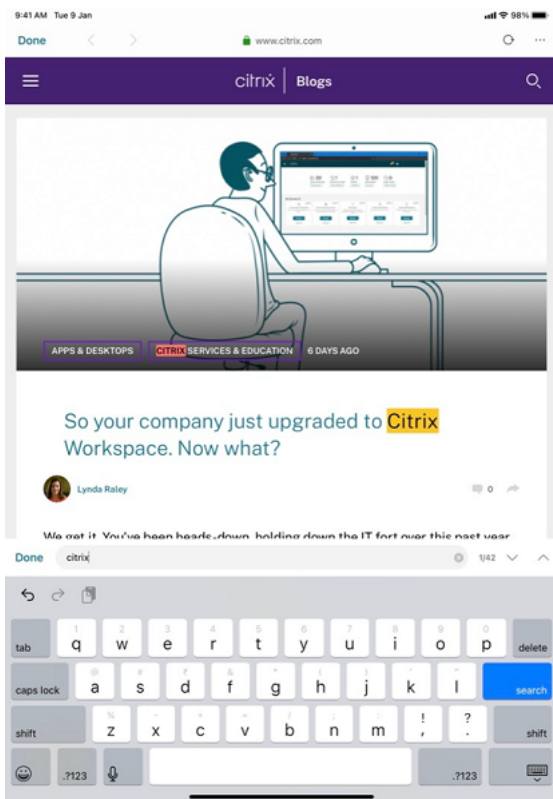
## Aplicación Citrix Workspace para iOS



Aparece el teclado en pantalla.



1. Escriba el texto que quiere buscar en el cuadro de texto (por ejemplo, escriba la palabra “Citrix”). Aparecerán los resultados de la búsqueda.



### Reposicionar la barra de herramientas de la sesión

Puede cambiar la posición de la barra de herramientas de la sesión en la parte superior o a la derecha de la pantalla. Al arrastrar la muesca de la barra de herramientas fuera del borde de la barra de herramientas, aparecen el indicador de arrastre rectangular y dónde soltarla. Suelte ahí el indicador de arrastre para cambiar la posición de la barra de herramientas.

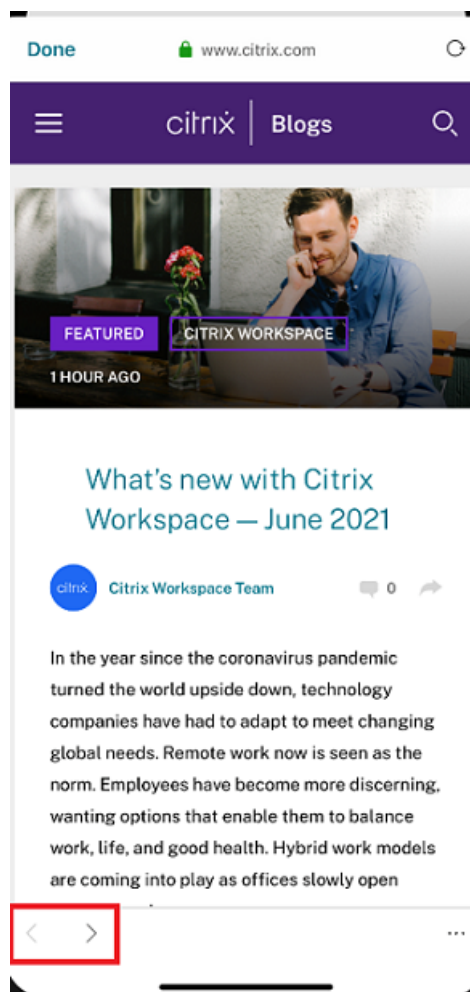
#### Notas:

- La función solo se aplica a usuarios de iPad.
- La función funciona con toques o con el mouse.
- La función funciona con un iPad o en una pantalla externa.
- La última posición de la barra de herramientas persiste en el inicio de la siguiente sesión o aplicación.

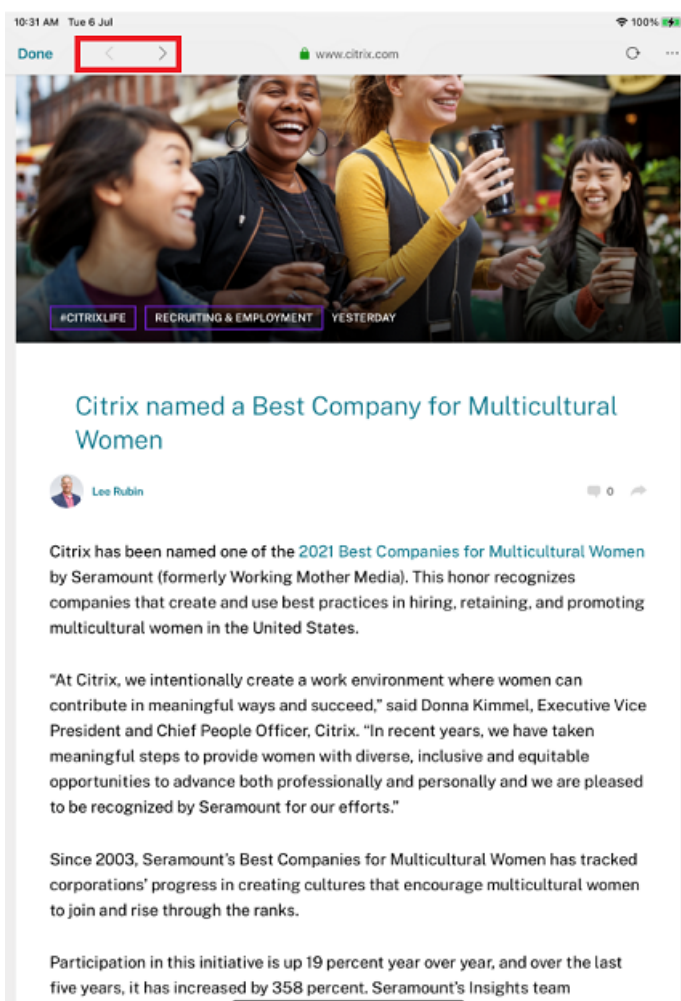
## Cambiar entre aplicaciones SaaS y web

La mejora de usabilidad permite navegar hacia adelante y hacia atrás en las aplicaciones web y SaaS.

Los botones de navegación aparecen en la parte inferior izquierda de las sesiones de las aplicaciones SaaS y web de Workspace de su iPhone.



Los botones de navegación aparecen en la parte superior izquierda de las sesiones de las aplicaciones SaaS y web de Workspace del iPad.



### Migración de una cuenta local a una cuenta de la nube

Los administradores pueden migrar fácilmente a los usuarios finales de una URL de almacén de Store-Front local a una URL de Workspace. Los administradores pueden realizar la migración con una interacción mínima del usuario final mediante [Global App Configuration Service](#).

Para llevar a cabo la configuración:

1. Vaya a la URL de [Global App Configuration Store Settings API](#) e introduzca la URL del almacén. Por ejemplo, `https://discovery.cem.cloud.us/ads/root/url/<hash coded store URL>/product/workspace/os/ios`.
2. Vaya **API Exploration > SettingsController > postDiscoveryApiUsingPOST** > y haga clic en **POST**.
3. Haga clic en **INVOKE API**.

4. Introduzca y cargue los detalles de la carga útil. Introduzca la fecha de caducidad del almacén de StoreFront en la marca de tiempo de epoch en milisegundos.

Por ejemplo,

```
1  "migrationUrl": [  
2  {  
3  
4  
5  "url": "<cloud store url>"  
6  "StoreFrontValidUntil": "<epoch timestamp in milliseconds>",  
7  }  
8  
9  ] ,  
10 <!--NeedCopy-->
```

5. Haga clic en **EXECUTE** para enviar el servicio.

### Experiencia de usuario final

Como usuario final, si utiliza la aplicación Citrix Workspace por primera vez, después de una autenticación correcta, aparece la pantalla de migración **Presentación del nuevo Citrix Workspace** (si cumple los requisitos). Después de tocar la opción **Probar el nuevo Citrix Workspace**, comienza la migración. Si la migración se realiza correctamente, puede acceder al almacén de Workspace (almacén de la nube).

#### Nota:

Puede omitir la migración tres veces. Luego, la migración se aplica sin que se pueda omitir.



Después de migrar al almacén (de la nube) de Workspace, puede ver tanto el almacén de StoreFront

como el almacén de Workspace en **Parámetros**. Cuando cambia de un almacén de la nube al almacén local de StoreFront, aparece una pantalla de comentarios para recopilar su respuesta.

**Nota:**

El almacén de StoreFront tiene fecha de caducidad. Una vez transcurrida la fecha de caducidad, el almacén se elimina.

## Integración con Siri

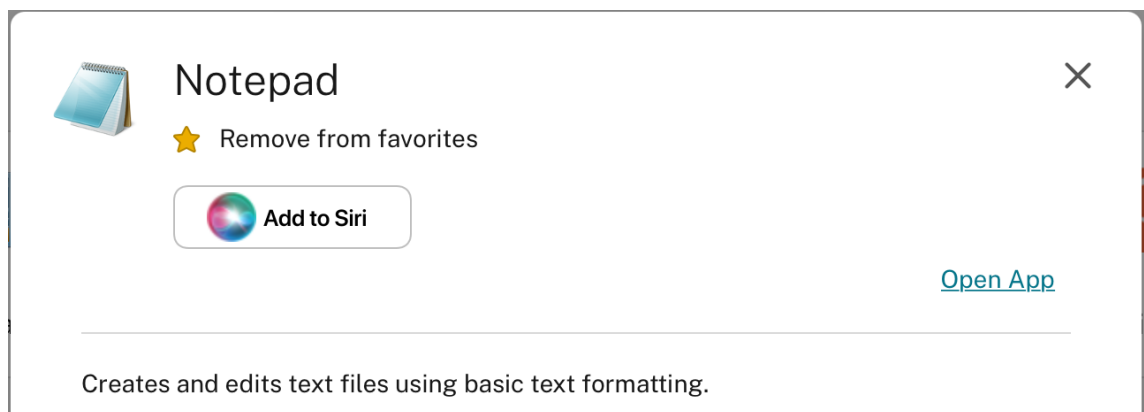
Puede interactuar con Siri para iniciar recursos como aplicaciones y escritorios sin tener que iniciar la aplicación Citrix Workspace cada vez.

### Para configurar

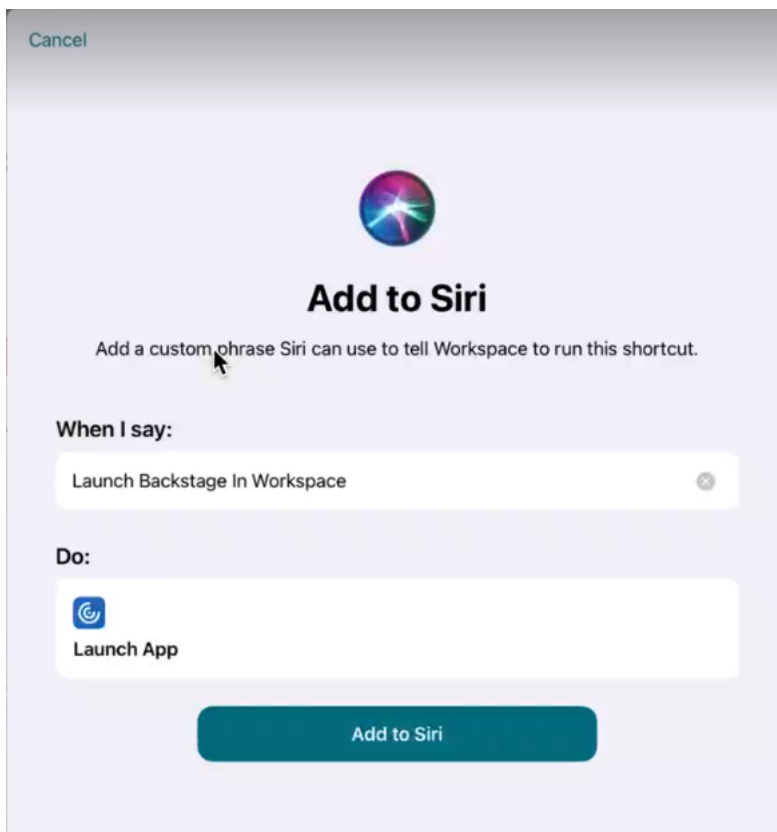
1. Inicie la aplicación Citrix Workspace y toque **Aplicaciones** o **Escritorios**. Seleccione el recurso que quiera agregar al acceso directo de Siri.
2. Toque puntos suspensivos (...). Aparecerá un cuadro de diálogo.

**Nota:**

Si es usuario de escritorio de iPhone o iPad, toque **puntos suspensivos (...)** > **Detalles de la aplicación** > **Ver detalles**. Aparecerá un cuadro de diálogo. Continúe con el paso 3.



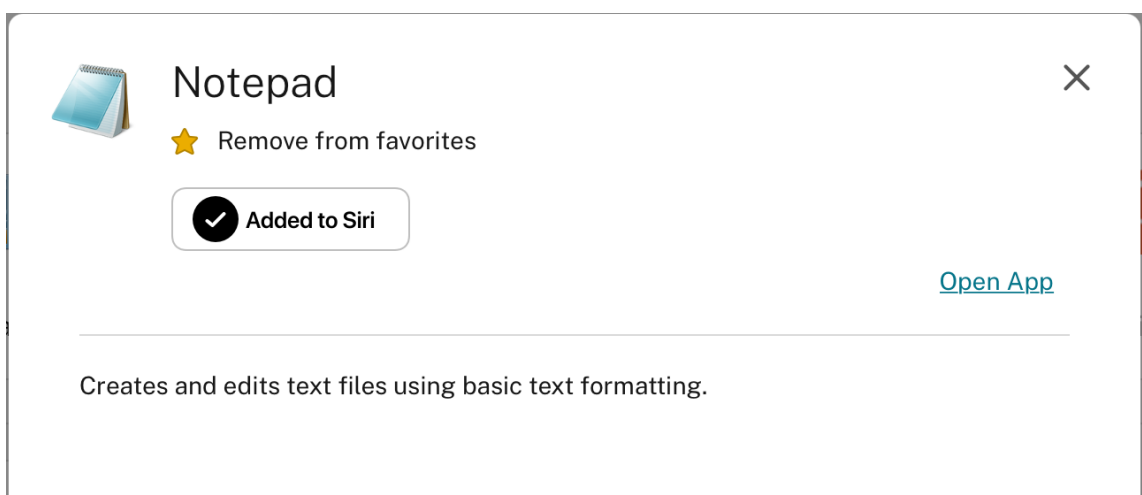
3. Toque **Agregar a Siri**. Aparecerá el cuadro de diálogo **Agregar a Siri**.



4. (Opcional) Modifique la frase personalizada para llamar a Siri. Toque **Agregar a Siri**. El recurso se agregará ahora al acceso directo de Siri. Cierre el cuadro de diálogo.

**Nota:**

Algunos dispositivos admiten la grabación de la frase personalizada para invocar Siri.





## Parámetros de la aplicación

Inicie la aplicación Citrix Workspace y toque el icono de su perfil > **Parámetros de la aplicación** > **Configuración de Siri**. Para activar la función, toque **Agregar a Siri**.

Ahora puede usar su voz para iniciar el recurso.

## Para modificar o eliminar el acceso directo

1. Seleccione el recurso.
2. Toque puntos suspensivos (...). Aparecerá un cuadro de diálogo.
3. Toque **Se agregó a Siri**. Aparecerá el cuadro de diálogo **Modificar acceso directo**.

## Compatibilidad con ventanas de sesión independientes de la aplicación Citrix Workspace

A partir de la versión 24.1.0, la aplicación Citrix Workspace para iOS presenta una ventana de sesión independiente que hace que la multitarea sea más eficiente y fácil de usar. Con esta función, puede disfrutar de una experiencia similar a la de un escritorio. Cuando la función Ventana de sesión independiente está habilitada, simplemente puede arrastrar y colocar las sesiones en los monitores externos conectados. De esta forma, el monitor principal del iPad se puede usar en modo multitarea con otras aplicaciones.

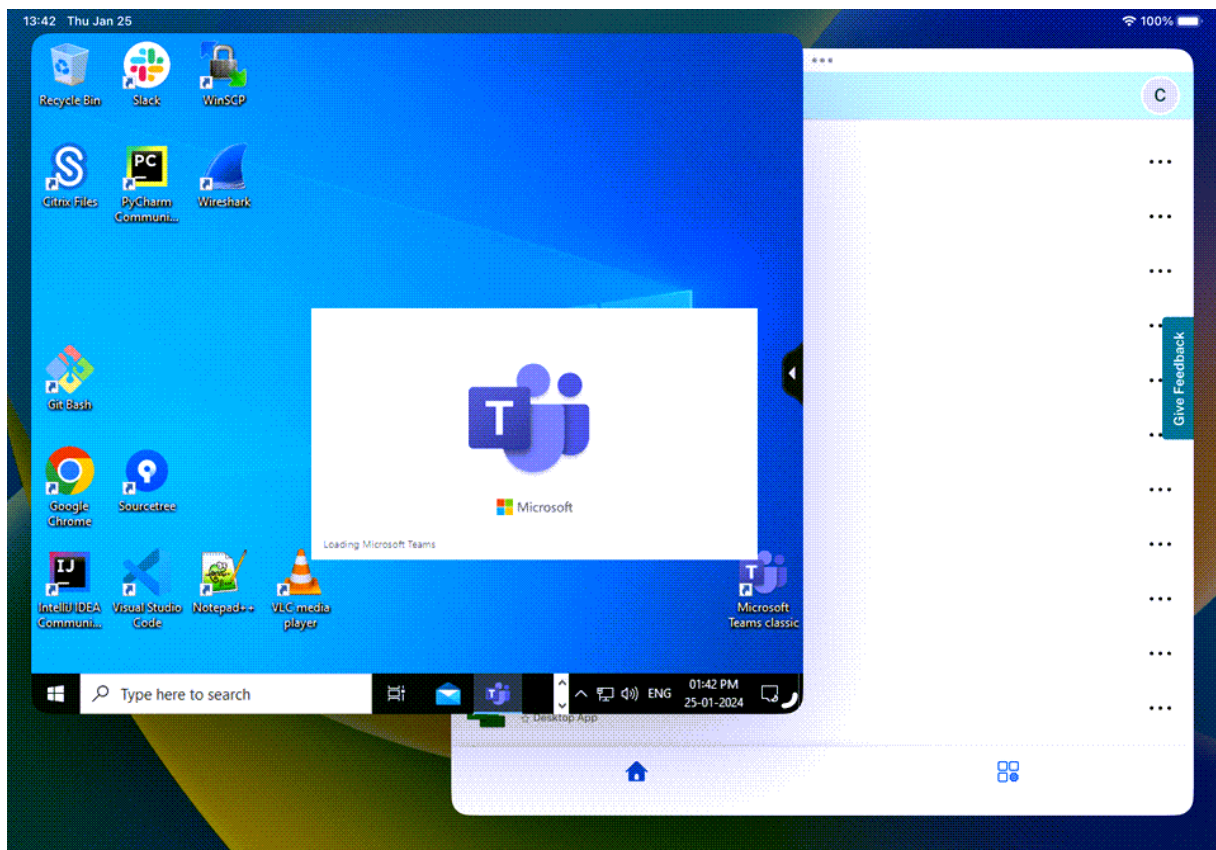
Esta función incluye las siguientes mejoras:

- Al hacer clic en el botón **Inicio** de la barra de menús de la sesión, se abre la ventana de la interfaz de usuario de Citrix Workspace en lugar de cerrarse la ventana de la sesión HDX. Esta mejora le permite usar la interfaz de usuario de Citrix Workspace y la sesión HDX al mismo tiempo. Si inicia una nueva sesión desde la interfaz de usuario de Citrix Workspace, la sesión existente se desconecta automáticamente.
- Al hacer clic en el botón **Apariencia** de la barra de menús de la sesión, aparece una ventana de configuración en la parte superior de la sesión HDX. Esta ventana le permite ajustar la resolución de la sesión en lugar de los parámetros de la interfaz de usuario de Citrix Workspace.

### Nota:

Esta función solo es compatible en los dispositivos que admiten la función Organizador visual. Todos los dispositivos iPhone y algunos dispositivos iPad no admiten esta función. Para obtener más información sobre la función Organizador visual, consulte [Activar o desactivar el organizador visual en el iPad](#) en la documentación de asistencia de Apple.

Para configurar la función de ventana de sesión independiente, vaya a **Parámetros** -> **Avanzados** -> **Multitarea** y seleccione **Ventana de sesión independiente**.



## Vista web para aplicaciones web y SaaS

March 28, 2024

### Página web

#### Uso compartido externo de páginas web

Puede compartir con otros usuarios las páginas web que abra desde la aplicación Citrix Workspace. Puede hacer lo siguiente:

- Copiar enlaces desde una vista web
- Abrir páginas web directamente en Safari
- Enviar enlaces directamente a usuarios o aplicaciones

Para compartir, toque el icono ... de la parte superior derecha de la vista web o mantenga pulsado cualquier enlace dentro de la vista web y toque la opción que necesite.

## **Vista web**

### **Vista web mejorada con controles nativos para aplicaciones SaaS**

Puede obtener una vista web mejorada con controles nativos para aplicaciones SaaS. Esta mejora permite:

- Ver la URL de las aplicaciones.
- Ver la información de seguridad de las aplicaciones.
- Compartir las aplicaciones.

Además, ahora puede deslizar el dedo hacia la izquierda y hacia la derecha sobre las aplicaciones para avanzar y retroceder, respectivamente.

### **Visor web de aplicaciones móviles de Citrix Workspace**

El visor web es una solución de navegación integrada en la aplicación que se ejecuta en la aplicación Citrix Workspace. Permite a los usuarios abrir aplicaciones web o SaaS desde la aplicación Citrix Workspace de forma segura. El visor web garantiza una interfaz de usuario uniforme al acceder a distintas aplicaciones web o SaaS. Mejora la productividad y ofrece un mejor rendimiento en la representación de las aplicaciones.

Con un enfoque continuo en enriquecer la experiencia de usuario, el nuevo visor web le ofrece una experiencia mejorada y más nativa con estas funciones:

- Acceso sin VPN a páginas web internas
- SSO para web y SaaS con directivas de acceso adaptable
- Descarga de archivos con vista previa
- Navegación integrada entre páginas y sitios
- Capacidad para compartir direcciones URL
- Buscar en la página
- vista uniforme al acceder a enlaces a través del feed de actividades

Los administradores pueden habilitar Secure Private Access (SPA), incluidos la descarga, el portapapeles, las restricciones de navegación, la carga de archivos y las marcas de agua, en distintas combinaciones según las URL.

## **Administración de contraseñas**

March 28, 2024

## Guardar contraseñas

Mediante la consola de administración de la Interfaz Web de Citrix, puede configurar el método de autenticación para permitir que los usuarios guarden sus contraseñas. Cuando se configura la cuenta de usuario, la contraseña cifrada se guarda hasta que el usuario se conecta por primera vez. Se deben tener en cuenta las siguientes cuestiones:

- Si se habilita el almacenamiento de contraseñas, la aplicación Citrix Workspace para iOS almacena la contraseña en el dispositivo para inicios de sesión futuros y ya no se solicitan las contraseñas cuando los usuarios se conectan con las aplicaciones.

### Nota:

La contraseña se almacena solamente si los usuarios introducen una contraseña cuando se crea una cuenta. Si no se introduce una contraseña para la cuenta, no se guarda ninguna contraseña, independientemente de cómo se haya configurado este parámetro en el servidor.

- Si se inhabilita el almacenamiento de contraseñas (configuración predeterminada), la aplicación Citrix Workspace para iOS solicita a los usuarios que introduzcan sus contraseñas cada vez que se conectan.

### Nota:

Para conexiones directas con StoreFront, no es posible guardar la contraseña.

## Para anular el parámetro de almacenamiento de contraseñas

Si se configura el servidor para que almacene las contraseñas, los usuarios que prefieran que les sean solicitadas las mismas cada vez que inician una sesión pueden anular dicho parámetro:

- Al crear la cuenta, deje el campo de contraseña en blanco.
- Al modificar la cuenta, elimine la contraseña y guarde la cuenta.

## Cómo utilizarlo

La aplicación Citrix Workspace tiene una función que simplifica el proceso de conexión, ya que permite guardar la contraseña, lo que elimina el paso adicional de tener que autenticar una sesión cada vez que se abre la aplicación.

### Nota:

Actualmente, la funcionalidad de **Guardar contraseñas** admite el protocolo PNA. No admite el modo *nativo* de StoreFront. Sin embargo, esta funcionalidad está operativa cuando StoreFront

habilita el modo *antiguo* de PNA.

## Configurar StoreFront para guardar la contraseña

Para configurar StoreFront para habilitar la funcionalidad de **Guardar contraseñas**:

1. Si configura un almacén existente, vaya al paso 3.
2. Para configurar una nueva implementación de StoreFront, siga la prácticas recomendadas descritas en [Instalación, configuración, actualización de versiones y desinstalación](#).
3. Abra la consola de administración de Citrix StoreFront. Asegúrese de que la URL base usa HTTPS y es la misma que el nombre común especificado al generar el certificado SSL.
4. Seleccione el almacén que quiere configurar.
5. Haga clic en **Configurar soporte de servicios XenApp**.
6. Habilite la **compatibilidad con el servicio XenApp**, seleccione el **almacén predeterminado** (opcional) y haga clic en **Aceptar**.
7. Vaya al archivo de plantilla de configuración, que se encuentra en `c:\inetpub\wwwroot\Citrix\<nombre del almacén>\Views\PnaConfig\`.
8. Haga una copia de seguridad del archivo Config.aspx.
9. Abra el archivo Config.aspx.
10. Modifique la línea `<EnableSavePassword>false</EnableSavePassword>` para cambiar el valor **false** a **true**.
11. Guarde el archivo Config.aspx modificado.
12. En el servidor de StoreFront, ejecute PowerShell con derechos de administrador.
13. En la consola PowerShell:
  - a. `cd "c:\\Program Files\\Citrix\\Receiver StoreFront\\Scripts"`
  - b. Escriba "Set-ExecutionPolicy RemoteSigned"
  - c. Escriba ".\ImportModules.ps1"
  - d. Escriba "Set-DSServiceMonitorFeature -ServiceUrl"https://localhost:443/StoreFrontMonitor"
14. Si tiene un grupo de StoreFront, ejecute los mismos comandos en todos los miembros del grupo.

## Configurar Citrix Gateway para guardar contraseñas

### Nota:

Esta configuración usa servidores de equilibrio de carga de Citrix Gateway.

Para configurar Citrix Gateway con el objetivo de ofrecer la funcionalidad de contraseñas guardadas:

1. Inicie sesión en la consola de administración de Citrix Gateway.
2. Siga la práctica recomendada por Citrix para crear un certificado para los servidores virtuales de equilibrio de carga.
3. En la ficha de configuración, vaya a **Traffic Management > Load Balancing > Servers** y haga clic en **Add**.
4. Introduzca el nombre y la dirección IP del servidor de StoreFront.
5. Haga clic en **Crear**. Si tiene un grupo de StoreFront, repita el paso 5 en cada uno de los servidores del grupo.
6. En la ficha de configuración, vaya a **Traffic Management -> Load Balancing -> Monitor** y haga clic en **Add**.
7. Introduzca un nombre para el monitor. Seleccione **StoreFront** como tipo (Type). En la parte inferior de la página, seleccione **Secure** (es necesario porque el servidor de StoreFront usa HTTPS).
8. Haga clic en la ficha **Special Parameters**. Introduzca el nombre de StoreFront configurado anteriormente, seleccione **Check Backed Services** y haga clic en **Create**.
9. En la ficha **Configuration**, vaya a **Traffic Management > Load Balancing > Service Groups** y haga clic en **Add**.
10. Introduzca un nombre para el grupo de servicios, establezca el protocolo en **SSL** y haga clic en **OK**.
11. En la parte derecha de la pantalla, en la sección Advanced Settings, seleccione **Settings**.
12. Habilite la IP de cliente, introduzca lo siguiente como valor de encabezado: **X-Forwarded-For** y haga clic en **OK**.
13. En la parte derecha de la pantalla, en la sección Advanced Settings, seleccione **Monitors**. Haga clic en la flecha para agregar nuevos monitores.
14. Haga clic en el botón **Add** y, a continuación, seleccione el menú desplegable **Select Monitor**. Aparecerá una lista de monitores (configurados en Citrix Gateway).
15. Haga clic en el botón de opción situado junto al monitor que creó anteriormente y haga clic en **Select** y, a continuación, en **Bind**.

16. En la parte derecha de la pantalla (en la sección Advanced Settings), seleccione **Members**. Haga clic en la flecha para agregar nuevos miembros del grupo de servicios.
17. Haga clic en el botón **Add** y, a continuación, seleccione la lista desplegable **Select Member**.
18. Seleccione el botón de opción **Server Based**. Aparecerá una lista de miembros del servidor (configurados en Citrix Gateway). Haga clic en el botón de opción junto al servidor de StoreFront que creó anteriormente.
19. Introduzca 443 como número de puerto y especifique un número exclusivo para el ID de hash. A continuación, haga clic en **Create** y en **Done**. Si todo se ha configurado correctamente, en **Effective State** aparecerá una luz verde, lo que indica que la supervisión está funcionando adecuadamente.
20. Vaya a **Traffic Management -> Load Balancing -> Virtual Servers** y haga clic en **Add**. Introduzca un nombre para el servidor y seleccione **SSL** como protocolo.
21. Introduzca la dirección IP del servidor de StoreFront de carga equilibrada y haga clic en **OK**.
22. Seleccione el vínculo **Load Balancing Virtual Server Service Group**, haga clic en la flecha y agregue el grupo de servicios creado previamente. Haga clic en **OK** dos veces.
23. Asigne el certificado SSL creado para el servidor virtual de equilibrio de carga. Seleccione **No Server Certificate**.
24. Seleccione el certificado del servidor de equilibrio de carga en la lista y haga clic en **Bind**.
25. Agregue el certificado de dominio al servidor de equilibrio de carga. Haga clic en **No CA certificate**.
26. Seleccione el certificado de dominio y haga clic en **Bind**.
27. En el lado derecho de la pantalla, seleccione **Persistence**.
28. Cambie el valor de Persistence a **SOURCEIP** y establezca el tiempo de espera en **20**. Haga clic en **Save** y luego en **Done**.
29. En el servidor DNS del dominio, agregue el servidor de equilibrio de carga (si aún no se ha creado).
30. Inicie la aplicación Citrix Workspace para iOS en el dispositivo iOS e introduzca la URL completa de XenApp.

## Autenticación

July 1, 2024

## Autenticación de certificados de cliente

### Importante:

- Cuando se utiliza StoreFront, la aplicación Citrix Workspace admite:
  - Citrix Access Gateway Enterprise Edition 9.3
  - NetScaler Gateway de la versión 10.x a la versión 11.0
  - Citrix Gateway 11.1 y versiones posteriores
- La aplicación Citrix Workspace para iOS admite la autenticación con certificados del cliente.
- Solo Access Gateway Enterprise Edition 9.x y 10.x (y versiones posteriores) admiten la autenticación con certificados del cliente.
- Los tipos de autenticación de doble origen deben ser CERT y LDAP.
- La aplicación Citrix Workspace también admite la autenticación opcional con certificados del cliente.
- Solo se admiten certificados con formato P12.

Los usuarios que inician sesiones en un servidor Citrix Gateway virtual pueden ser autenticados también basándose en los atributos del certificado del cliente que se presenta ante el servidor virtual. La autenticación con certificados del cliente también puede utilizarse con otro tipo de autenticación, LDAP, para ofrecer autenticación de doble origen.

Los administradores pueden autenticar a los usuarios finales basándose en los atributos del certificado del lado del cliente de la siguiente manera:

- La autenticación de clientes está habilitada en el servidor virtual.
- El servidor virtual solicita un certificado de cliente.
- Para enlazar un certificado raíz al servidor virtual en Citrix Gateway.

Cuando los usuarios inician sesión en el servidor Citrix Gateway virtual, después de la autenticación, pueden extraer el nombre de usuario y la información del dominio del campo **SubjectAltName:OtherName:MicrosoftUniversalPrincipalName** del certificado. Está en el formato `username@domain`.

La autenticación se completa cuando el usuario extrae el nombre de usuario y el dominio, y proporciona la información necesaria (como la contraseña). Si el usuario no presenta un certificado y credenciales válidas, o si falla la extracción del nombre de usuario y el dominio, la autenticación también fallará.

Se puede autenticar usuarios basándose en el certificado del cliente, definiendo el tipo de autenticación predeterminado para que use el certificado del cliente. También se puede crear una acción de certificado que defina lo que hay que hacer durante la autenticación basada en un certificado SSL del cliente.



## Para configurar la comunidad de XenApp

Cree una comunidad de XenApp para dispositivos móviles en la consola de Citrix Virtual Apps o en la consola de Interfaz Web. La consola depende de la versión de Citrix Virtual Apps que haya instalado.

La aplicación Citrix Workspace usa una comunidad de XenApp para obtener información acerca de las aplicaciones sobre las que tiene derechos un usuario. La misma información se comparte con las aplicaciones que se ejecutan en el dispositivo. Este método es similar al modo en que se utiliza la Interfaz Web para las conexiones tradicionales de Citrix Virtual Apps basadas en SSL, en las que se puede configurar un dispositivo Citrix Gateway.

Configure la comunidad de XenApp para que la aplicación Citrix Workspace para dispositivos móviles sea compatible con conexiones procedentes de Citrix Gateway de la siguiente manera:

1. En la comunidad de XenApp, seleccione **Manage secure client access > Edit secure client access settings**.
2. Cambie el método de acceso a Direct con Gateway.
3. Escriba el nombre de dominio completo del dispositivo Citrix Gateway.
4. Escriba la información de Secure Ticket Authority (STA).

## Para configurar el dispositivo Citrix Gateway

La autenticación con el certificado del cliente requiere configurar Citrix Gateway con la autenticación de dos factores mediante las directivas de autenticación Cert y LDAP. Para configurar el dispositivo Citrix Gateway:

1. Cree una directiva de sesión en Citrix Gateway para permitir las conexiones entrantes de Citrix Virtual Apps desde la aplicación Citrix Workspace y especifique la ubicación de la comunidad de XenApp recién creada.
  - Cree una directiva de sesión nueva para identificar que la conexión proviene de la aplicación Citrix Workspace. Al crear la directiva de sesión, configure la siguiente expresión y elija Hacer coincidir todas las expresiones como el operador de la expresión:  
`REQ.HTTP.HEADER User-Agent CONTAINS CitrixWorkspace`
  - En la configuración del perfil asociado para la directiva de sesión, en la ficha **Security**, configure **Default Authorization** con el valor **Allow**(Permitir).

En la ficha **Published Applications**, si no es un parámetro global (es decir, la casilla “Override Global” está marcada), compruebe que el campo **ICA Proxy** esté **activado**.

En el campo **Address** de la Interfaz Web, introduzca la URL, incluido config.xml, de la comunidad de XenApp que utilizan los usuarios del dispositivo, por ejemplo:

- /NombreServidorXenApp/Citrix/PNAgent/config.xml
    - o
  - /NombreServidorXenApp/RutaPersonalizada/config.xml.
- Vincule la directiva de sesión con un servidor virtual.
  - Cree directivas de autenticación para Cert y LDAP.
  - Vincule las directivas de autenticación con el servidor virtual.
  - Configure el servidor virtual para solicitar certificados del cliente en la negociación de la conexión TLS. Para hacerlo, vaya a **Certificate > abra SSL Parameters > Client Authentication >** y establezca **Client Certificate** en **Mandatory**.

#### Importante:

Si el certificado del servidor que se usa en Citrix Gateway forma parte de una cadena de certificados. Por ejemplo, si se trata de un certificado intermedio, instale los certificados en Citrix Gateway. Para obtener más información sobre la instalación de certificados, consulte la documentación de Citrix Gateway.

### Para configurar el dispositivo móvil

Si la autenticación de certificados del cliente está habilitada en Citrix Gateway, los usuarios se autenticarán basándose en ciertos atributos del certificado del cliente. Tras la autenticación, puede extraer el nombre de usuario y el dominio del certificado. Puede aplicar directivas específicas para cada usuario.

1. En la aplicación Citrix Workspace, abra la **Cuenta** y, en el campo Servidor, escriba el FQDN correspondiente de su servidor de Citrix Gateway. Por ejemplo, ServidorCertificadosClienteGateway.empresa.com. La aplicación Citrix Workspace detecta automáticamente que se necesita el certificado del cliente.
2. Los usuarios pueden instalar un certificado nuevo o bien seleccionar uno de la lista de certificados ya instalados. Para la autenticación de certificados del cliente iOS, descargue e instale el certificado solo desde la aplicación Citrix Workspace.
3. Después de seleccionar un certificado válido, los campos correspondientes al nombre de usuario y dominio de la pantalla de inicio de sesión se rellenan automáticamente con el nombre de usuario del certificado. El usuario final puede introducir otros detalles, incluida la contraseña.
4. Si la autenticación con certificado del cliente es optativa, los usuarios pueden omitir la selección de certificado. Para ello, deberán presionar el botón Atrás en la página de certificados. En este caso, la aplicación Citrix Workspace continúa con la conexión y presenta al usuario la pantalla de inicio de sesión.

- Una vez que los usuarios completan el inicio de sesión, pueden iniciar las aplicaciones sin tener que proporcionar el certificado nuevamente. La aplicación Citrix Workspace almacena el certificado de la cuenta y lo utiliza automáticamente para solicitudes de inicio de sesión futuras.

### Configurar la directiva de reescritura para el proceso de autenticación

Los administradores pueden cambiar el explorador web que se utiliza para el proceso de autenticación del explorador web integrado al explorador web del sistema. Esto solo es posible al configurar una directiva de autenticación avanzada en la implementación local de Citrix Gateway y StoreFront. Para configurar una directiva de autenticación avanzada, configure la directiva de reescritura de NetScaler mediante la línea de comandos de NetScaler:

- `enable ns feature REWRITE`
- `add rewrite action insert_auth_browser_type_hdr_act insert_http_header X-Auth-WebBrowser "\"System\""`
- `add rewrite policy insert_auth_browser_type_hdr_pol "HTTP.REQ.URL.EQ(\"/cgi/authenticate\")"insert_auth_browser_type_hdr_act`
- `bind vpn vserver <VPN-vserver-Name> -policy insert_auth_browser_type_hdr_pol -priority 10 -gotoPriorityExpression END -type AAA_RESPONSE`

Al pasar al explorador web del sistema, dispone de más prestaciones, tales como:

- Mejor experiencia con la autenticación basada en certificados.
- Posibilidad de utilizar un certificado de usuario existente del almacén de claves del dispositivo durante el proceso de autenticación.
- Compatibilidad con algunos autenticadores de terceros, como SITHS eID.

El explorador web integrado se utiliza como explorador web predeterminado para la autenticación si el administrador no ha configurado la directiva de reescritura mencionada.

En esta tabla se enumeran los exploradores web que se utilizan para la autenticación según la configuración de NetScaler Gateway y Global App Config Service:

| NetScaler Gateway | Global App Configuration Service | Explorador web utilizado para la autenticación |
|-------------------|----------------------------------|------------------------------------------------|
| Sistema           | Sistema                          | Sistema                                        |
| Sistema           | Integrado                        | Sistema                                        |
| Integrado         | Sistema                          | Sistema                                        |
| Integrado         | Integrado                        | Integrado                                      |
| Sin configuración | Sistema                          | Sistema                                        |

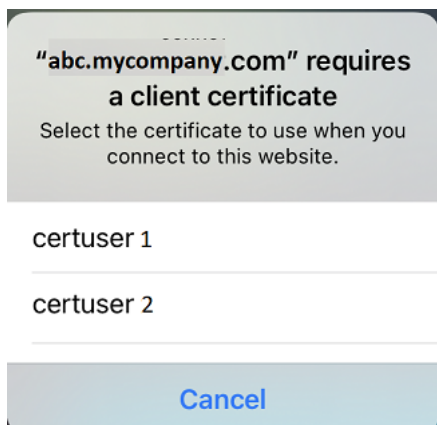
|                   |                                  |                                                |
|-------------------|----------------------------------|------------------------------------------------|
| NetScaler Gateway | Global App Configuration Service | Explorador web utilizado para la autenticación |
| Sin configuración | Integrado                        | Integrado                                      |

### Función de autenticación basada en certificados para almacenes locales

Los usuarios finales ahora pueden gestionar la autenticación por certificado, y los certificados se guardan en el llavero del dispositivo. Al iniciar sesión, la aplicación Citrix Workspace detecta la lista de certificados del dispositivo y se puede elegir un certificado para la autenticación.

**Importante:**

Al elegir un certificado, la opción elegida se conserva la siguiente vez que se inicia la aplicación Citrix Workspace. Para elegir otro certificado, puede “restablecer Safari” desde la configuración del dispositivo iOS o volver a instalar la aplicación Citrix Workspace.



**Nota:**

Esta funcionalidad admite implementaciones locales.

Para llevar a cabo la configuración:

1. Vaya a la URL de [Global App Configuration Store Settings API](#) e introduzca la URL del almacén. Por ejemplo, `https://discovery.cem.cloud.us/ads/root/url/<hash coded store URL>/product/workspace/os/ios`.
2. Vaya **API Exploration > SettingsController > postDiscoveryApiUsingPOST >** y haga clic en **POST**.
3. Haga clic en **INVOKE API**.
4. Introduzca y cargue los detalles de la carga útil. Seleccione uno de los valores siguientes:

- “Embedded”: Puede usar WKWebView. Esta es la opción predeterminada.
- “system”: Puede usar el controlador de vistas de Safari.

Por ejemplo,

```
1 "category": "Authentication",
2 "userOverride": false,
3 "settings": [
4 {
5   "name": "Web Browser to use for Authentication", "value": "*
   Embedded*/*System*" }
6 ,
7 <!--NeedCopy-->
```

En los dispositivos iOS o iPad, los administradores pueden cambiar el explorador web que se utiliza para el proceso de autenticación. Puede cambiar del explorador web integrado al explorador web del sistema si configura una directiva de autenticación avanzada en la implementación local de Citrix Gateway y StoreFront. Para obtener más información, consulte Configurar la directiva de reescritura para el proceso de autenticación.

5. Haga clic en **EXECUTE** para enviar el servicio.

## Tarjetas inteligentes

La aplicación Citrix Workspace admite el uso de tarjetas inteligentes SITHS solo en conexiones dentro de la sesión.

Si usa dispositivos Citrix Gateway FIPS, configure sus sistemas para rechazar renegociaciones SSL. Para obtener información detallada, consulte el artículo [CTX123680](#) de Knowledge Center.

Se admiten los productos y las configuraciones siguientes:

- Lectores admitidos:
  - Precise Biometrics Tactivo para iPad Mini Firmware versión 3.8.0
  - Precise Biometrics Tactivo para iPad (cuarta generación) y Tactivo para iPad (tercera generación) y la versión 3.8.0 del firmware del iPad 2
  - Lectores de tarjeta inteligente BaiMobile® 301MP y 301MP-L
  - Lector USB Thursby PKard
  - Lector USB Feitian iR301
  - Lectores compatibles con CCID tipo C
  - lector de la utilidad para tarjetas inteligentes twocanoes
- Compatibilidad con middleware de tarjeta inteligente para VDA
  - ActiveIdentity

- Tarjetas inteligentes admitidas:
  - Tarjetas PIV
  - Tarjetas CAC (Common Access Card)
- Configuraciones admitidas:
  - Autenticación con tarjeta inteligente en Citrix Gateway con StoreFront 2.x y XenDesktop 7.x o versiones posteriores, o XenApp 6.5 o versiones posteriores

### Cómo configurar la aplicación Citrix Workspace para acceder a las aplicaciones

1. Si quiere configurar la aplicación Citrix Workspace automáticamente para acceder a aplicaciones al crear una cuenta, introduzca la URL de su almacén en el campo “Dirección”. Por ejemplo:
  - StoreFront.empresa.com
  - netscalervserver.empresa.com
2. Seleccione la opción **Usar tarjeta inteligente** cuando vaya a utilizar una tarjeta inteligente para la autenticación.

#### **Nota:**

Los inicios de sesión en un almacén son válidos durante una hora aproximadamente. Transcurrido ese tiempo, los usuarios tienen que iniciar de nuevo una sesión para actualizar o iniciar sus aplicaciones.

### Compatibilidad con el lector de la utilidad para tarjetas inteligentes twocanoes

A partir de la versión 24.3.5, la aplicación Citrix Workspace para iOS admite los lectores de la utilidad para tarjetas inteligentes twocanoes. Para obtener más información acerca de los lectores de tarjetas inteligentes compatibles, consulte [Tarjetas inteligentes](#).

#### **Nota:**

El lector USB-C de la utilidad para tarjetas inteligentes twocanoes es compatible tanto para el inicio de sesión virtual como para el inicio de sesión con la aplicación Citrix Workspace. Sin embargo, el lector Bluetooth de la utilidad para tarjetas inteligentes twocanoes solo es compatible con el inicio de sesión en la aplicación Citrix Workspace, y no con el inicio de sesión virtual.

Para configurar el lector Bluetooth de la utilidad para tarjetas inteligentes twocanoes, siga estos pasos:

1. Descargue e instale la aplicación Smart Card Utility en el App Store. Para obtener más información, consulte [Smart Card Utility Bluetooth Reader Quick Star](#) en la base de conocimientos de twocanoes.
2. Asegúrese de que la función Bluetooth del dispositivo esté activada y de que la tarjeta inteligente se haya introducido en el lector.
3. Abra la aplicación Smart Card Utility.



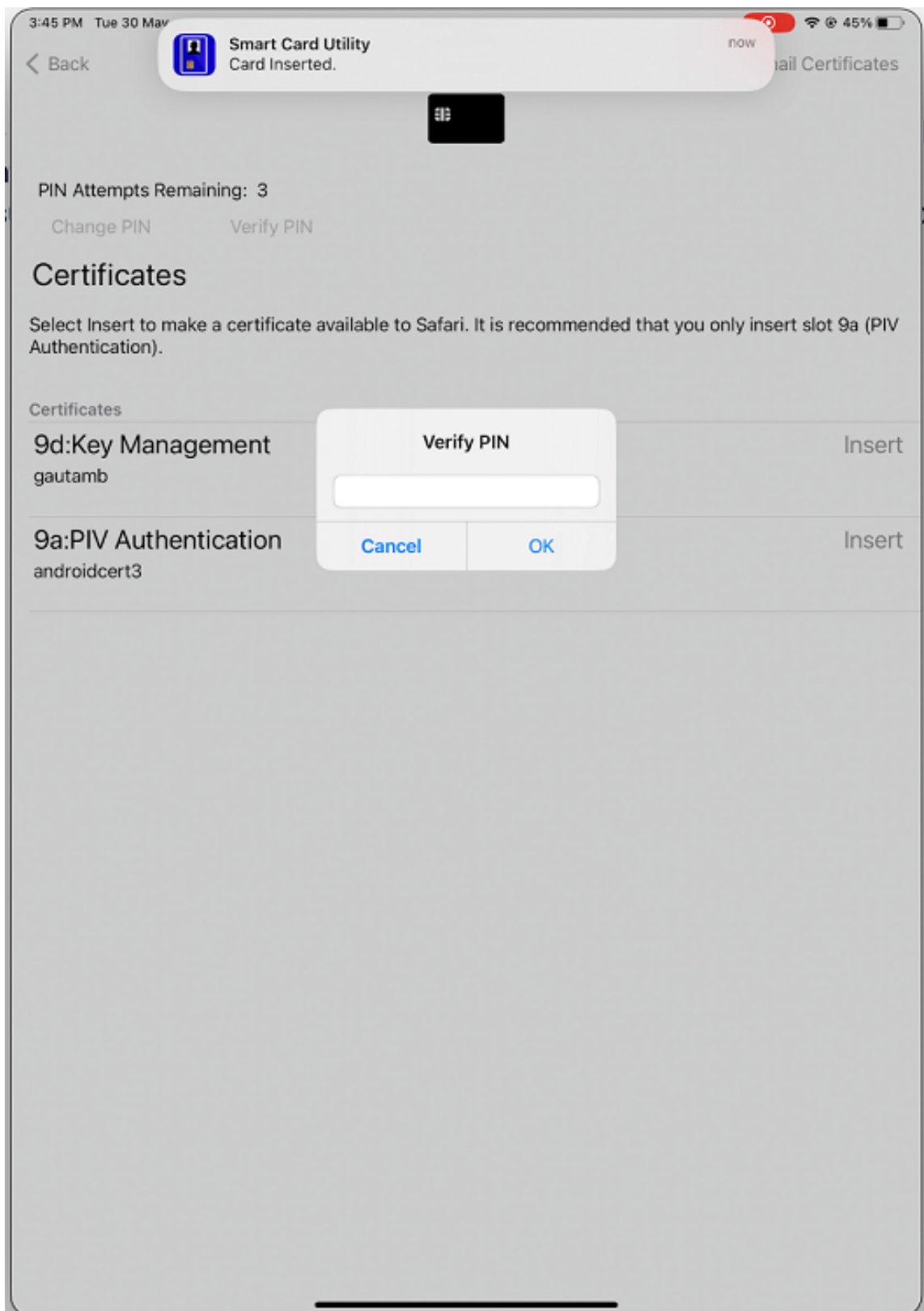
4. Si usa el lector Bluetooth, toque **Add Bluetooth or Other Reader...** y seleccione el lector para



conectarlo.

**Nota:**

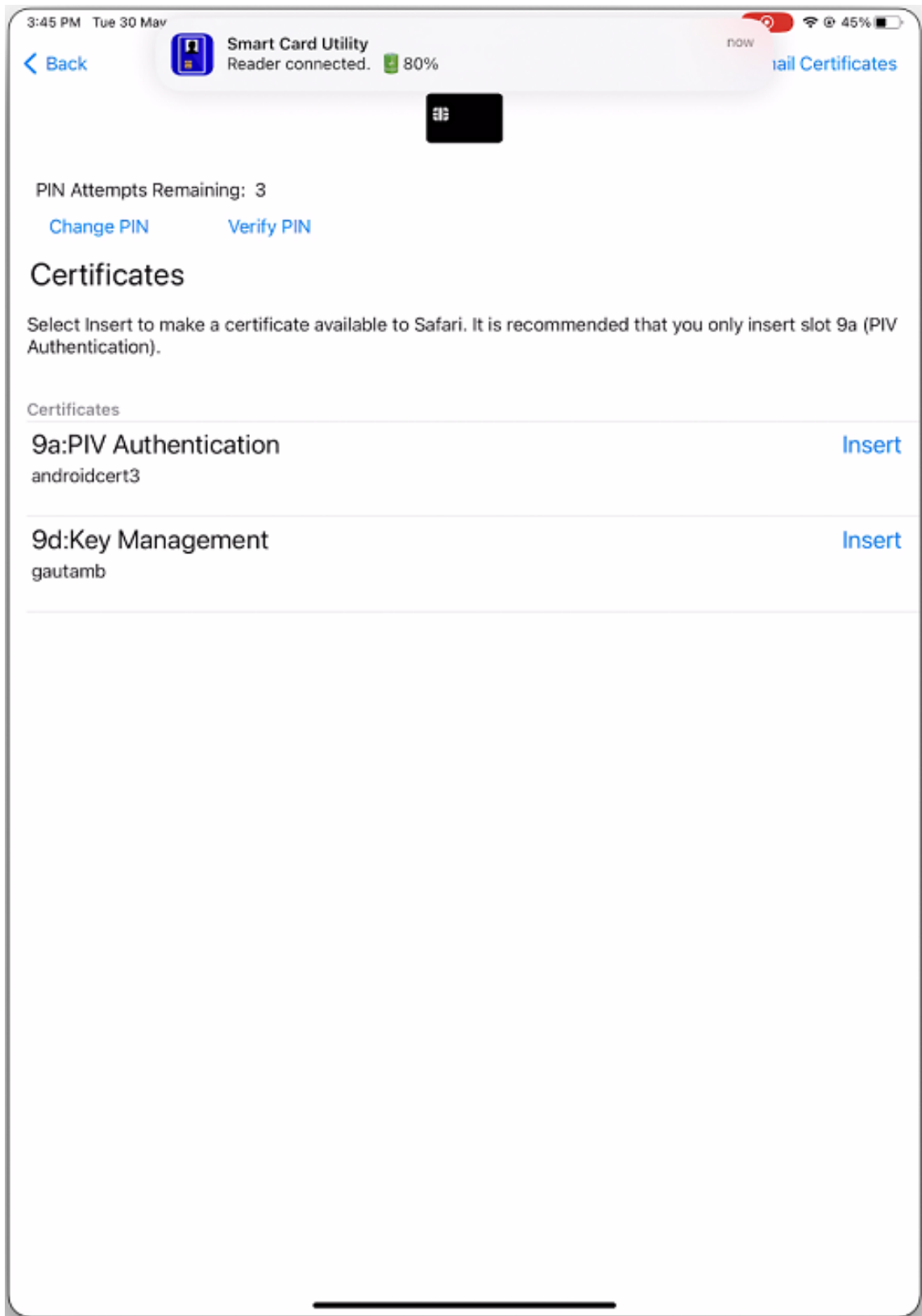
Si el lector está habilitado para el emparejamiento de PIN, debe introducir el **PIN** cuando se le indique. El **PIN** está disponible en la parte posterior del lector.



5. Toque **Insert** en el certificado requerido para copiarlo en la interfaz del llavero.

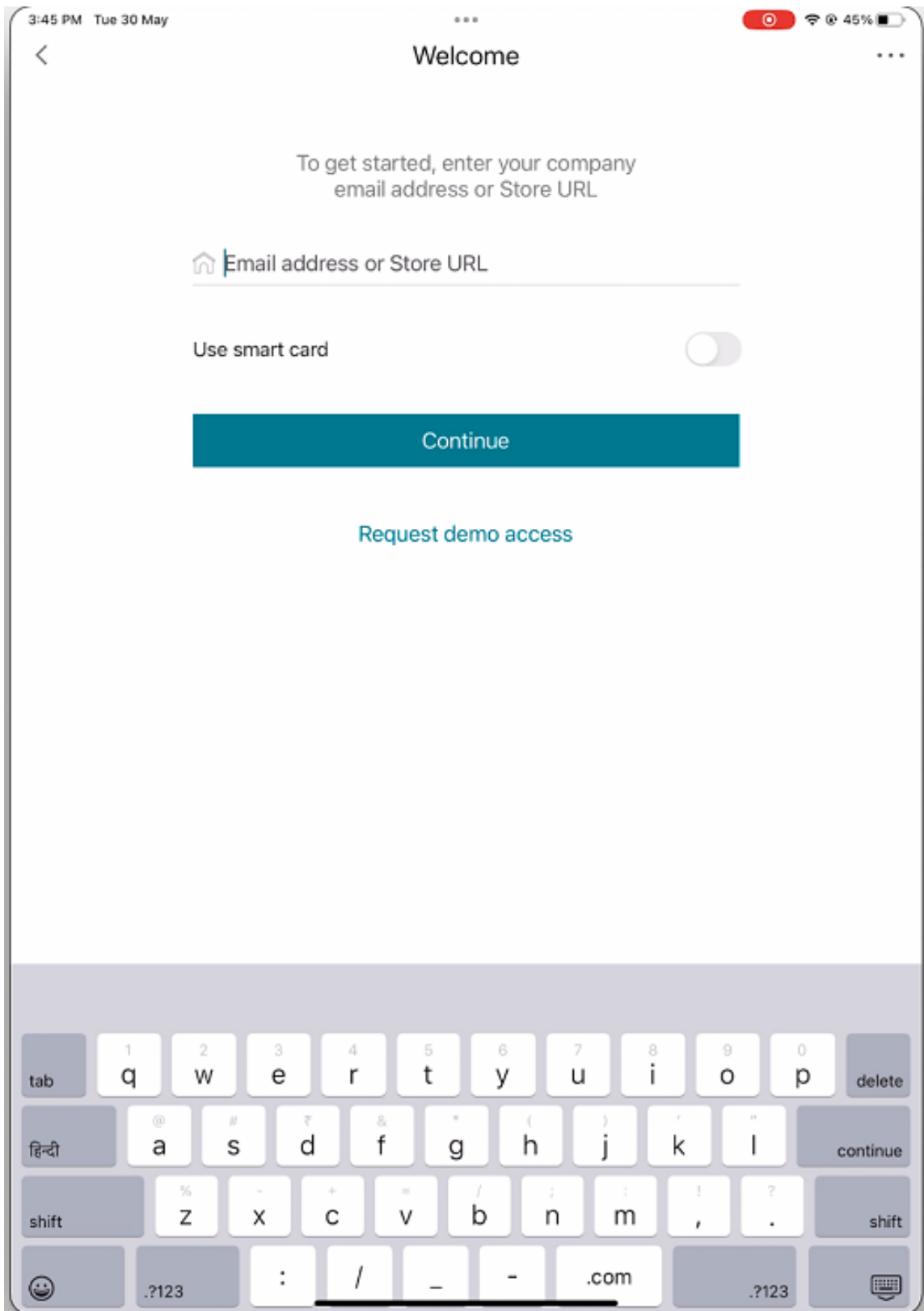
**Nota:**

La aplicación Smart Card Utility ha implementado una extensión cryptokit proporcionada por Apple para escribir certificados en la interfaz del llavero en forma de tokens. Para obtener más información, consulte [Configure Smart Card Authentication](#) en la documentación para desarrolladores de Apple.

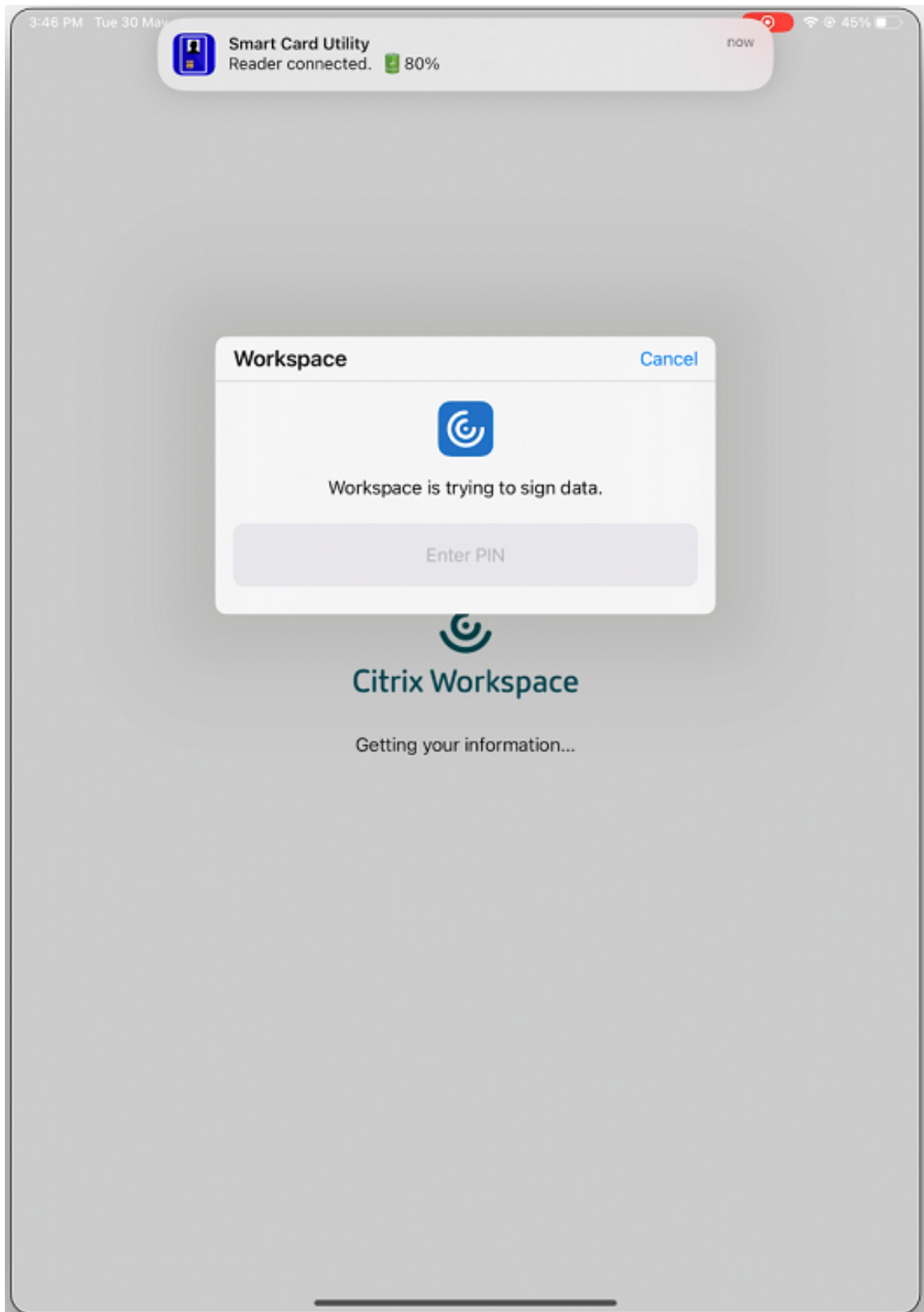


6. Asegúrese de que el lector permanece conectado al dispositivo.

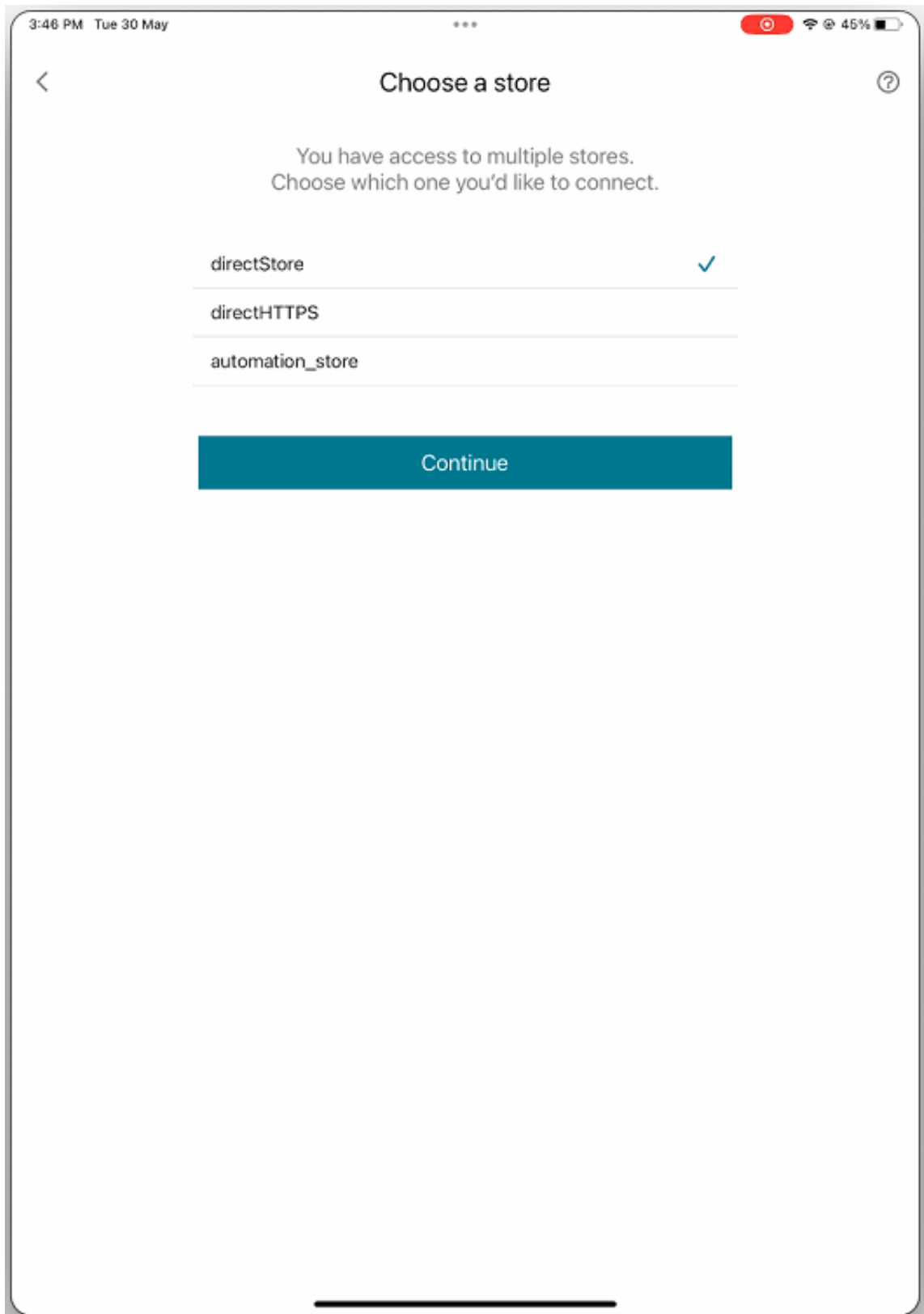
7. Abra la aplicación Citrix Workspace e introduzca la URL del almacén configurado con autenticación con tarjeta inteligente.



8. En la pantalla Certificados, seleccione el certificado requerido e introduzca el PIN de la tarjeta inteligente que le proporcionó el administrador de TI para iniciar sesión.



9. Si tiene acceso a varios almacenes, seleccione el almacén requerido y toque **Continue**.



10. Tras la autenticación, habrá iniciado sesión en la aplicación Citrix Workspace.



## **Compatibilidad con YubiKey para la autenticación con tarjeta inteligente**

Ahora puede realizar la autenticación con tarjeta inteligente con YubiKey. Esta función proporciona una experiencia de autenticación de un solo dispositivo para la aplicación Citrix Workspace y para las sesiones virtuales y las aplicaciones publicadas en la sesión del VDA. Elimina la necesidad de conectar lectores de tarjetas inteligentes u otros autenticadores externos. Simplifica la experiencia del usuario final, ya que YubiKey es compatible con una amplia variedad de protocolos, como OTP, FIDO, etc.

Para iniciar sesión en la aplicación Citrix Workspace, los usuarios finales deben insertar la YubiKey en su iPhone o iPad, activar la opción de tarjeta inteligente y proporcionar su URL del almacén.

### **Nota:**

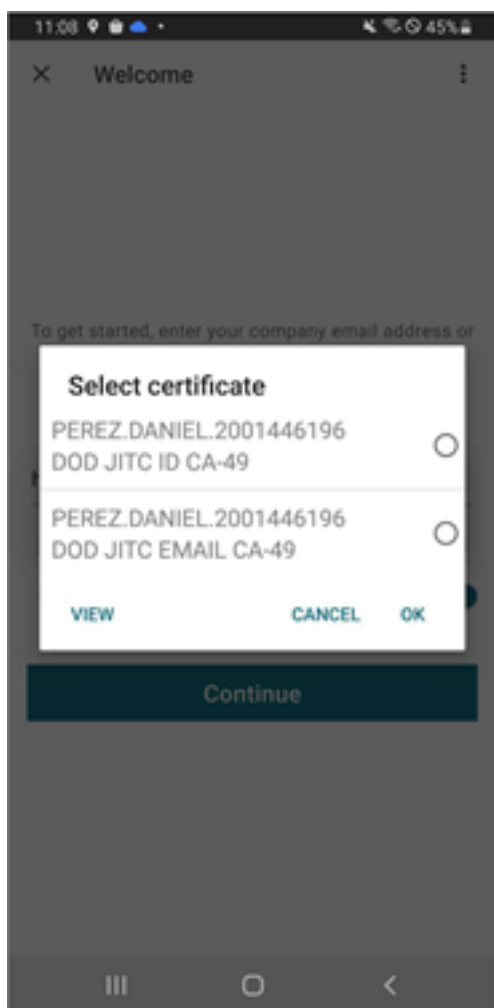
Esta función solo admite la conexión directa a la aplicación Citrix Workspace en las implementaciones de StoreFront y no a través de Citrix Gateway. La compatibilidad de YubiKey con la autenticación con tarjetas inteligentes a través de Citrix Gateway estará disponible en una versión próxima.

La aplicación Citrix Workspace para iOS solo admite la serie YubiKey 5. Para obtener más información sobre YubiKey, consulte la [serie YubiKey 5](#).

## **Compatibilidad con varios certificados en la autenticación con tarjeta inteligente**

Anteriormente, la aplicación Citrix Workspace para iOS mostraba el certificado disponible en la primera ranura de la tarjeta inteligente conectada.

A partir de la versión 24.1.0, la aplicación Citrix Workspace para iOS muestra todos los certificados disponibles en la tarjeta inteligente. Esta función le permite seleccionar el certificado requerido durante la autenticación mediante tarjeta inteligente.



### Autenticación con RSA SecurID

La aplicación Citrix Workspace admite la autenticación RSA SecurID en las configuraciones de Secure Web Gateway. Las configuraciones se realizan a través de la Interfaz Web y para todas las configuraciones de Citrix Gateway.

**Se requiere un esquema de URL para el token de software en la aplicación Citrix Workspace para iOS:** El token de software de RSA SecurID usado por la aplicación Citrix Workspace registra solamente el esquema de URL `com.citrix.securid`.

Si los usuarios han instalado las aplicaciones Citrix Workspace y RSA SecurID en sus dispositivos iOS, deberán seleccionar el esquema de URL **`com.citrix.securid`** para importar el token de software de RSA SecurID en los dispositivos con la aplicación Citrix Workspace.

### Para importar un token de software de RSA SecurID

Para usar un token de software de RSA con la aplicación Citrix Workspace, como administrador, asegúrese de que los usuarios finales respeten lo siguiente:

- la directiva sobre longitud del PIN
- el tipo de PIN (solo numérico y alfanumérico)
- los límites de reutilización del PIN

Una vez que el usuario final se ha autenticado correctamente en el servidor RSA, solo tiene que configurar el PIN una vez. Después de la verificación del PIN, se autentican también en el servidor StoreFront. Después de toda la verificación, la aplicación Workspace muestra las aplicaciones y los escritorios disponibles y publicados.

### Para utilizar un token de software de RSA

1. Importe el token de software de RSA suministrado por su organización.
2. En el mensaje que lleva adjunto el archivo de SecurID, seleccione **Abrir en Workspace** como destino de la importación. Después de importar el token de software, la aplicación Citrix Workspace se abre automáticamente.
3. Si su organización le proporcionó una contraseña para completar la importación, introdúzcala y haga clic en **Aceptar**. Al hacer clic en **Aceptar**, aparecerá un mensaje donde se indica que el token se ha importado.
4. Cierre el mensaje de importación y, en la aplicación Citrix Workspace, toque en **Agregar cuenta**.
5. Introduzca la dirección URL del almacén que le haya facilitado su organización y haga clic en **Siguiente**.
6. En la pantalla de inicio de sesión, escriba sus credenciales (nombre de usuario, contraseña y dominio). En el campo PIN, introduzca **0000**, a menos que su organización le haya facilitado otro PIN predeterminado. El PIN 0000 es el predeterminado de RSA, pero es posible que su organización lo cambie por otro, para cumplir con sus directivas de seguridad.
7. En la parte superior izquierda, haga clic en **Iniciar sesión**. Aparecerá un mensaje para crear un PIN.
8. Introduzca un PIN de entre 4 y 8 dígitos y haga clic en **Aceptar**. Aparecerá un mensaje para verificar el nuevo PIN.
9. Vuelva a introducir el PIN y haga clic en **Aceptar**. Ahora puede acceder a sus aplicaciones y escritorios.

## Siguiente tokencode

Si configura Citrix Gateway para la autenticación con RSA SecurID, la aplicación Citrix Workspace admite la funcionalidad siguiente tokencode. Si introduce tres contraseñas incorrectas, aparece un mensaje de error en el plug-in de Citrix Gateway. Para iniciar sesión, espere al siguiente token. Asimismo, el servidor RSA se puede configurar para inhabilitar una cuenta de usuario si el usuario intenta iniciar una sesión demasiadas veces con la contraseña incorrecta.

## Credenciales derivadas

Las credenciales derivadas de Purebred dentro de la aplicación Citrix Workspace están disponibles. Al conectarse a un almacén que permite credenciales derivadas, los usuarios pueden iniciar sesión en la aplicación Citrix Workspace con una tarjeta inteligente virtual. Esta función solo está disponible en implementaciones locales.

### Nota:

Para usar esta función, se requiere Citrix Virtual Apps and Desktops 7 1808 o versiones posteriores.

Para habilitar las credenciales derivadas en la aplicación Citrix Workspace:

1. Vaya a **Parámetros > Avanzado > Credenciales derivadas**.
2. Toque **Credenciales derivadas**.

Para crear una tarjeta inteligente virtual que admita credenciales derivadas:

1. En **Parámetros > Avanzado > Credenciales derivadas**, toque **Agregar nueva tarjeta inteligente virtual**.
2. Modifique el nombre de la tarjeta inteligente virtual.
3. Introduzca un PIN de solo 8 dígitos numéricos y confírmelo.
4. Toque **Siguiente**.
5. En Certificado de autenticación, toque **Importar certificado...**
6. Aparece el selector de documentos. Toque **Examinar**.
7. En Ubicaciones, seleccione **Llavero de Purebred**.
8. Seleccione el certificado de autenticación adecuado de la lista.
9. Toque **Importar clave**.
10. Repita los pasos 5 a 9 para el Certificado de firma digital y el Certificado de cifrado, si quiere.
11. Toque **Guardar**.

Puede importar tres certificados, como máximo, para su tarjeta inteligente virtual. El certificado de autenticación es necesario para que la tarjeta inteligente virtual funcione correctamente. El certificado de cifrado y el certificado de firma digital se pueden agregar para usarlos en una sesión VDA.

**Nota:**

Al conectarse a una sesión HDX, la tarjeta inteligente virtual creada se redirige a la sesión.

**Limitaciones conocidas**

- Los usuarios solo pueden tener una tarjeta activa a la vez.
- Una vez que se ha creado una tarjeta inteligente virtual, no se puede modificar. Elimínela y cree otra tarjeta.
- Puede introducir un máximo de diez veces un PIN no válido. Si no es válido después de diez intentos, la tarjeta inteligente virtual se elimina.
- Al seleccionar credenciales derivadas, la tarjeta inteligente virtual anula una tarjeta inteligente física.

**Cadena de usuario-agente para WKWebView**

De forma predeterminada, la cadena de usuario-agente utilizada durante algunas de las solicitudes de red iniciadas a través de WKWebView incluye ahora el identificador de la aplicación Citrix Workspace.

Por lo tanto, se ha cambiado de:

```
Mozilla/5.0 (iPhone; CPU iPhone OS 15_2 like Mac OS X) AppleWebKit  
/605.1.15 (KHTML, like Gecko) Mobile/15E148 AuthManager/3.2.4.0
```

A una de las siguientes opciones:

```
Mozilla/5.0 (iPhone; CPU iPhone OS 15_0 like Mac OS X) AppleWebKit  
/605.1.15 (KHTML, like Gecko) Mobile/15E148 CWA/23.3.0 iOS/15.0  
X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPhone  
(iPhone de ejemplo)
```

O bien,

```
Mozilla/5.0 (iPhone; CPU iPhone OS 15_0 like Mac OS X) AppleWebKit  
/605.1.15 (KHTML, like Gecko) Mobile/15E148 CWA/23.3.0 iOS/15.0  
X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPad  
(iPad de ejemplo)
```

## Autenticación nFactor

### Compatibilidad con autenticación de varios factores (nFactor)

La autenticación de varios factores mejora la seguridad de las aplicaciones porque requiere que los usuarios proporcionen varias pruebas de identificación para obtener acceso. La autenticación de varios factores hace que el administrador pueda configurar los pasos de autenticación y los formularios de recopilación de credenciales asociados.

La aplicación Citrix Workspace nativa puede admitir este protocolo a partir de la funcionalidad de formularios de inicio de sesión ya implementada para StoreFront. La página de inicio de sesión web de los servidores virtuales de Citrix Gateway y Traffic Manager también utiliza este protocolo.

Para obtener más información, consulte [Autenticación SAML](#) y [Autenticación de varios factores \(nFactor\)](#).

#### Limitaciones:

- Con la autenticación nFactor habilitada, no se puede utilizar autenticación biométrica como Touch ID y Face ID.

### Compatibilidad con directivas de autenticación avanzada nFactor

Ahora admitimos la autenticación por certificados en la aplicación Citrix Workspace cuando se configura mediante las directivas de autenticación avanzada nFactor en Citrix Gateway. La autenticación nFactor permite configurar esquemas flexibles y ágiles de varios factores.

#### Cadena de usuario-agente:

Al realizar la autenticación avanzada (nFactor) para la aplicación Citrix Workspace en un iPhone o un iPad, el proceso de autenticación se redirige a un WebView integrado. La cadena de agente de usuario resultante podría variar ligeramente según la versión del sistema operativo, la versión de compilación de CWA, el modelo de dispositivo y la versión de AuthManager. Por ejemplo, considere las siguientes cadenas de agente de usuario para iPhone y iPad.

Para iPhone:

```
Mozilla/5.0 (iPhone; CPU iPhone OS 16_2 like Mac OS X) AppleWebKit  
/605.1.15 (KHTML, like Gecko) Mobile/15E148 CWA/23.5.0 iOS/16.2  
X1Class CWACapable 302RedirectionCapable CFNetwork Darwin CWA-iPhone  
AuthManager/3.3.0.0
```

Para iPad:

```
Mozilla/5.0 (Macintosh; Intel Mac OS X 10_15_6) AppleWebKit/605.1.15 (  
KHTML, like Gecko) Mobile/15E148 CWA/23.5.0 iOS/15.0 X1Class CWACapable
```

302RedirectionCapable CFNetwork Darwin CWA-iPad AuthManager/3.3.0.0

Esta función se encuentra en Tech Preview. Se puede habilitar mediante solicitud a través del [enlace de Podio](#) o poniéndose en contacto con la asistencia técnica de Citrix. Sin embargo, eventualmente se extenderá a todos los clientes una vez finalizado el plazo de Technical Preview.

**Nota:**

- Es posible que la información sobre la versión o el modelo del dispositivo varíen según el entorno.
- Para aplicar directivas basadas en agente de usuario específicas de la aplicación Citrix Workspace para iOS durante la autenticación, use las siguientes palabras clave:
  - iOS
  - CWA
  - CWACapable

### **Compatibilidad con la autenticación basada en FIDO2 al conectarse a una sesión HDX**

La aplicación Citrix Workspace para iOS ahora admite la autenticación sin contraseña dentro de una sesión de Citrix Virtual Apps and Desktops mediante métodos de autenticación basados en FIDO2. Esta función permite a los usuarios iniciar sesión en un sitio web compatible con WebAuthn en exploradores como Google Chrome o Microsoft Edge mediante claves de seguridad Yubico compatibles con FIDO2. El simple hecho de abrir un sitio web compatible con WebAuthn desencadena la autenticación sin contraseña.

Solo se admiten dispositivos con puertos Lightning (no se admiten dispositivos con puertos USB-C o USB 4). No se admite el inicio de sesión en la aplicación Citrix Workspace o en la sesión de escritorio mediante autenticación sin contraseña.

Para obtener más información sobre los requisitos previos, consulte [Autorización local y autenticación virtual mediante FIDO2](#) en la documentación de Citrix Virtual Apps and Desktops.

### **Función de autenticación mediante FIDO2 al conectarse a almacenes de la nube**

A partir de la versión 24.5.0, los usuarios pueden autenticarse en la aplicación Citrix Workspace mediante la autenticación sin contraseña basada en FIDO2 al conectarse a almacenes de la nube. FIDO2 ofrece un método de autenticación integrado que permite a los empleados de la empresa acceder a aplicaciones y escritorios dentro de sesiones virtuales sin necesidad de introducir un nombre de usuario o una contraseña. Esta función admite tanto itinerancia (solo USB) como autenticadores de plataforma (código PIN, Touch ID y Face ID). Esta función está habilitada de manera predeterminada.

**Nota:**

De forma predeterminada, la autenticación FIDO2 es compatible con las fichas personalizadas de Chrome. Si le interesa usar la autenticación FIDO2 con WebView, registre su interés utilizando este [formulario de Podio](#).

## **Función para configurar el almacenamiento de tokens de autenticación en la implementación local**

La aplicación Citrix Workspace para iOS ofrece ahora una opción que permite configurar el almacenamiento de los tokens de autenticación en el disco local para los almacenes locales. Con esta función, puede inhabilitar el almacenamiento del token de autenticación para mejorar la seguridad. Tras la inhabilitación, cuando se reinicie el sistema o la sesión, tendrá que autenticarse de nuevo para acceder a la sesión.

Para inhabilitar el almacenamiento de los tokens de autenticación en la implementación local mediante el archivo de configuración de administración, haga lo siguiente:

1. Utilice un editor de texto para abrir el archivo web.config, que normalmente se encuentra en `C:\inetpub\wwwroot\Citrix\Roaming directory`.
2. Localice el elemento de la cuenta de usuario en el archivo (Store es el nombre de cuenta de la implementación).  
Por ejemplo: `<account id=... name="Store">`
3. Antes de la etiqueta `</account>`, vaya a las propiedades de esa cuenta de usuario y agregue lo siguiente:

```
1 <properties>
2 <property name="TokenPersistence" value="false" />
3 </properties>
4 <!--NeedCopy-->
```

A continuación, se muestra un ejemplo del archivo web.config:

```
1 <account id="#####" name="Store
2 Service"
3 description="" published="true" updaterType="None"
4 remoteAccessType="StoresOnly">
5 <annotatedServices>
6 <clear />
7 <annotatedServiceRecord serviceRef="1__Citrix_Store">
8 <metadata>
9 <plugins>
10 <clear />
11 </plugins>
12 <trustSettings>
13 <clear />
```



```
12         </trustSettings>
13         <properties>
14             <clear />
15             <property name="TokenPersistence" value="false"
16                 />
17         </properties>
18     </annotatedServiceRecord>
19 </annotatedServices>
20 <metadata>
21 <plugins>
22     <clear />
23 </plugins>
24 <trustSettings>
25     <clear />
26 </trustSettings>
27 <properties>
28 </properties>
29 </metadata>
30 </account>
31 <!--NeedCopy-->
```

## Protección

January 7, 2024

Para proteger la comunicación entre la comunidad de servidores y la aplicación Citrix Workspace, integre las conexiones a la comunidad de servidores con la ayuda de diversas tecnologías de seguridad, incluido Citrix Gateway.

### Nota:

Citrix recomienda utilizar Citrix Gateway para proteger las comunicaciones entre los servidores StoreFront y los dispositivos de los usuarios.

- Un servidor proxy SOCKS o un servidor proxy de seguridad (también conocido como servidor proxy seguro o servidor proxy HTTPS).

Se pueden usar servidores proxy para limitar el acceso hacia y desde la red, y para gestionar las conexiones entre la aplicación Citrix Workspace y los servidores. La aplicación Citrix Workspace admite protocolos de proxy seguro y SOCKS.

- Secure Web Gateway

Puede utilizar Secure Web Gateway junto con la Interfaz Web para proporcionar un punto de acceso único, seguro y cifrado a Internet para los servidores situados en las redes internas de la organización.

Puede utilizar Secure Web Gateway con Interfaz Web para proporcionar datos únicos, seguros y cifrados. Los servidores de las redes corporativas internas pueden acceder a los datos protegidos a través de Internet.

- Soluciones de Traspaso SSL con protocolos TLS (Transport Layer Security)
- Un firewall.

Los firewall o servidores de seguridad de red pueden permitir o bloquear los paquetes basándose en la dirección y el puerto de destino.

Si usa la aplicación Citrix Workspace a través de un firewall que asigna la dirección IP de red interna del servidor a una dirección de Internet externa (es decir, traducción de direcciones de red, NAT), configure la dirección externa.

### **Citrix Gateway**

Para permitir que los usuarios remotos se conecten a su implementación de Citrix Endpoint Management mediante Citrix Gateway, puede configurar los certificados para que funcionen con StoreFront. El método que se debe utilizar para habilitar el acceso depende de la edición de Citrix Endpoint Management existente en la implementación.

Si implementa Citrix Endpoint Management en la red, integre Citrix Gateway con StoreFront para permitir las conexiones de usuarios internos y usuarios remotos a StoreFront a través de Citrix Gateway. Con esta implementación, los usuarios pueden conectarse a StoreFront para acceder a las aplicaciones publicadas desde XenApp y a los escritorios virtuales desde XenDesktop. Los usuarios se pueden conectar mediante la aplicación Citrix Workspace.

### **Secure Web Gateway**

Este tema solo se aplica a entornos donde se usa la Interfaz Web.

Es posible usar Secure Web Gateway en modo Normal o en modo Relay (Traspaso) para proporcionar un canal de comunicaciones seguro entre la aplicación Citrix Workspace y el servidor. Si usa Secure Web Gateway en modo **Normal**, no es necesario configurar la aplicación Citrix Workspace. Verifique que los usuarios finales se conectan a través de la Interfaz Web.

La aplicación Citrix Workspace usa parámetros que se configuran de forma remota en el servidor de la Interfaz Web para conectarse con los servidores que ejecutan Secure Web Gateway.

Si se instala Secure Web Gateway Proxy en un servidor de una red segura, se puede utilizar Secure Web Gateway Proxy en modo de traspaso (Relay). Si se utiliza el modo de traspaso, el servidor Secure Web Gateway funciona como un proxy y es necesario configurar la aplicación Citrix Workspace para que use lo siguiente:

- El nombre de dominio completo (FQDN) del servidor de Secure Web Gateway.
- El número de puerto del servidor de Secure Web Gateway.

**Nota:**

La versión 2.0 de Secure Web Gateway no ofrece el modo de traspaso.

El nombre de dominio completo (FQDN) debe tener los siguientes tres componentes, consecutivamente:

- Nombre de host
- Dominio intermedio
- Dominio superior

Por ejemplo, `my_computer.example.com` es un nombre de dominio completo (FQDN), ya que contiene una secuencia de nombre de host (`my_computer`), dominio intermedio (`example`) y dominio superior (`com`). La combinación del dominio intermedio y del dominio superior (`example.com`) se denomina “nombre de dominio”.

## Servidor proxy

Los servidores proxy se usan para limitar el acceso hacia y desde una red, y para ocuparse de las conexiones entre la aplicación Citrix Workspace y los servidores. La aplicación Citrix Workspace admite tanto protocolos de proxy seguro como SOCKS.

La aplicación Citrix Workspace usa la configuración del servidor proxy para comunicarse con el servidor de Citrix Virtual Apps and Desktops. Los parámetros del servidor proxy se configuran de forma remota en el servidor de la Interfaz Web.

Cuando la aplicación Citrix Workspace se comunica con el servidor web, utiliza la configuración del servidor proxy. Configure los parámetros del servidor proxy para el explorador web predeterminado en el dispositivo de usuario según corresponda.

## Firewall

Los firewall o servidores de seguridad de red pueden permitir o bloquear los paquetes basándose en la dirección y el puerto de destino. Si se utiliza un firewall en el entorno, la aplicación Citrix Workspace debe poder comunicarse a través de este con el servidor web y el servidor Citrix. El firewall debe permitir el tráfico HTTP para la comunicación desde el dispositivo de usuario hacia el servidor Web. Por lo general, el tráfico HTTP se dirige a través del puerto HTTP estándar 80 o 443 si se utiliza un servidor web seguro. Para las comunicaciones del servidor Citrix, el firewall debe permitir el tráfico ICA entrante en los puertos 1494 y 2598.

Si el firewall se ha configurado para la traducción de direcciones de red (NAT), es posible usar la Interfaz Web para definir las asignaciones desde las direcciones internas hacia las direcciones externas y los puertos. Por ejemplo, si el servidor de Citrix Virtual Apps and Desktops y Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service) no se ha configurado con una dirección alternativa, puede configurar la Interfaz Web para proporcionar una dirección alternativa a la aplicación Citrix Workspace para iOS. A continuación, la aplicación Citrix Workspace para iOS se conecta con el servidor mediante la dirección externa y el número de puerto.

### TLS

La aplicación Citrix Workspace admite el uso de TLS 1.0, 1.1 y 1.2 con los siguientes conjuntos de cifrado para las conexiones TLS con XenApp y XenDesktop:

- TLS\_RSA\_WITH\_AES\_256\_GCM\_SHA384
- TLS\_RSA\_WITH\_AES\_128\_GCM\_SHA256
- TLS\_RSA\_WITH\_AES\_256\_CBC\_SHA
- TLS\_RSA\_WITH\_AES\_128\_CBC\_SHA
- TLS\_RSA\_WITH\_RC4\_128\_SHA
- TLS\_RSA\_WITH\_RC4\_128\_MD5
- TLS\_RSA\_WITH\_3DES\_EDE\_CBC\_SHA

#### Nota:

La aplicación Citrix Workspace en iOS 9 y versiones posteriores o la versión 21.2.0 no admiten estos conjuntos de cifrado TLS:

- TLS\_RSA\_WITH\_RC4\_128\_SHA
- TLS\_RSA\_WITH\_RC4\_128\_MD5

Transport Layer Security (TLS) es la versión estándar más reciente del protocolo TLS. La organización Internet Engineering Taskforce (IETF) le cambió el nombre a TLS al asumir la responsabilidad del desarrollo de TLS como un estándar abierto.

TLS protege las comunicaciones de datos mediante la autenticación del servidor, el cifrado del flujo de datos y la comprobación de la integridad de los mensajes. Algunas organizaciones, entre las que se encuentran organizaciones del gobierno de los EE. UU., requieren el uso de TLS para proteger las comunicaciones de datos. Es posible que estas organizaciones también exijan el uso de cifrado validado, como FIPS 140 (Federal Information Processing Standard). FIPS 140 es un estándar para cifrado.

La aplicación Citrix Workspace admite claves RSA de 1024, 2048 y 3072 bits. También se admiten certificados raíz con claves RSA de 4096 bits.

**Nota:**

- La aplicación Citrix Workspace usa criptografía de plataforma iOS para las conexiones entre la aplicación Citrix Workspace y StoreFront.

## Configurar y habilitar TLS

La configuración de TLS consta de dos pasos:

1. Configure el Traspaso SSL en el servidor de Citrix Virtual Apps and Desktops y en el servidor de la Interfaz Web. Obtenga e instale el certificado de servidor necesario.
2. Instale el certificado raíz equivalente en el dispositivo de usuario.

**Instalación de certificados raíz en los dispositivos de usuario** Para proteger las comunicaciones entre la aplicación Citrix Workspace con TLS y Citrix Virtual Apps and Desktops, necesita un certificado raíz en el dispositivo del usuario. El certificado puede verificar la firma de la entidad de certificación en el certificado del servidor.

iOS viene con cientos de certificados raíz comerciales preinstalados. Si quiere utilizar otro certificado, puede recibir uno de la entidad de certificación e instalarlo en cada dispositivo de usuario.

Según los procedimientos y las directivas de la empresa, puede instalar el certificado raíz en cada dispositivo de usuario en lugar de solicitar a los usuarios que lo instalen. La opción más fácil y segura es agregar los certificados raíz al llavero de iOS.

### Para agregar un certificado raíz a las llaves

1. Envíese un correo electrónico con el archivo del certificado.
2. Abra el archivo del certificado en el dispositivo. Esta acción inicia automáticamente la aplicación Acceso a Llaveros.
3. Siga las indicaciones para agregar el certificado.
4. A partir de iOS 10, compruebe que el certificado es de confianza desde **Ajustes de iOS > Información > Ajustes de confianza de los certificados**.

En Ajustes de confianza de los certificados, consulte la sección “Activar confianza total en los certificados raíz”. Compruebe que su certificado está seleccionado para la confianza total.

Se instalará el certificado raíz. Los clientes y otras aplicaciones habilitados para TLS pueden usar el certificado raíz con TLS.

## Sitio de XenApp y XenDesktop

Para configurar el sitio de XenApp y XenDesktop:

### Importante:

- La aplicación Citrix Workspace usa sitios de XenApp y XenDesktop, que son compatibles con Citrix Secure Gateway 3.x.
- La aplicación Citrix Workspace usa sitios web de Citrix Virtual Apps, que son compatibles con Citrix Secure Gateway 3.x.
- Los sitios de XenApp y XenDesktop solo admiten la autenticación de un factor.
- Los sitios web de Citrix Virtual Apps admiten la autenticación de un factor y de dos factores.
- Todos los exploradores web integrados son compatibles con la Interfaz Web 5.4.

Antes de comenzar esta configuración, instale y configure Citrix Gateway para que funcione con la Interfaz Web. Es posible adaptar estas instrucciones para que se adapten a su entorno específico.

Si utiliza una conexión de Citrix Secure Web Gateway, no configure Citrix Gateway en la aplicación Citrix Workspace.

La aplicación Citrix Workspace usa un sitio de XenApp y XenDesktop para obtener información acerca de las aplicaciones sobre las que tiene derechos un usuario final. En el proceso, la información se presenta a la aplicación Citrix Workspace que se ejecuta en el dispositivo. Del mismo modo, puede usar Interfaz Web para las conexiones tradicionales de Citrix Virtual Apps basadas en SSL. Para la misma conexión basada en SSL, puede configurar Citrix Gateway. Los sitios de XenApp y XenDesktop que se ejecutan en la Interfaz Web 5.x contienen esta capacidad de configuración.

Configure el sitio de XenApp y XenDesktop para que admita conexiones desde una conexión de Citrix Secure Gateway:

1. En el sitio de XenApp y XenDesktop, seleccione **Manage secure client access > Edit secure client access settings**.
2. Cambie el método de acceso a **Direct con Gateway**.
3. Escriba el FQDN de Secure Web Gateway.
4. Escriba la información de Secure Ticket Authority (STA).

### Nota:

Para Citrix Secure Gateway, Citrix recomienda usar la ruta predeterminada de Citrix (//Nombre-ServidorXenApp/Citrix/PNAgent). La ruta predeterminada permite a los usuarios finales especificar el FQDN de la instancia de Secure Web Gateway a la que se conectan. No utilice la ruta completa al archivo config.xml que se encuentra en el sitio de XenApp y XenDesktop. Por ejemplo: //XenAppServerName/CustomPath/config.xml.

### Para configurar Citrix Secure Gateway

1. Utilice el asistente de configuración de Citrix Secure Gateway para configurar la puerta de enlace.

Citrix Secure Gateway admite el servidor de la red segura que aloja el sitio de servicios XenApp. Después de seleccionar la opción **Indirecta**, introduzca la ruta del FQDN de su servidor de Secure Web Gateway y continúe con los pasos del asistente.

2. Pruebe la conexión desde un dispositivo de usuario para asegurarse de que Secure Web Gateway está configurado correctamente para la asignación de certificados y red.

### Para configurar el dispositivo móvil

1. Al agregar una cuenta de Citrix Secure Gateway, introduzca el nombre de dominio completo (FQDN) del servidor de Secure Gateway en el campo **Dirección**:

- Si ha creado el sitio de XenApp y XenDesktop con la ruta predeterminada (/Citrix/PNAgent), introduzca el FQDN de Secure Web Gateway: FQDNofSecureGateway.companyName.com
- Si personalizó la ruta del sitio de XenApp y XenDesktop, introduzca la ruta completa del archivo config.xml. Por ejemplo: FQDNofSecureGateway.companyName.com/CustomPath/config.xml

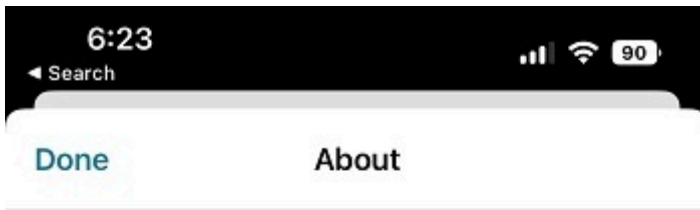
2. Si configura la cuenta manualmente, desactive la opción de Citrix Gateway en el cuadro de diálogo **Nueva cuenta**.

## Solucionar problemas técnicos

March 28, 2024

### Cómo comprobar la versión de la aplicación

Para comprobar la versión de la aplicación Citrix Workspace, abra la aplicación. Toque **Parámetros > Acerca de**. La información de la versión se muestra en la pantalla.



24.1.0.10 (2401)

© 1990-2024 Cloud Software Group, Inc.  
All Rights Reserved.

[Third Party Notices](#)

[User Agreements](#)





## **Cómo actualizar la aplicación Citrix Workspace a la versión más reciente**

Puede actualizar a la versión más reciente de la aplicación Citrix Workspace desde Apple Store. Busque la aplicación Citrix Workspace y toque el botón **Actualizar**.

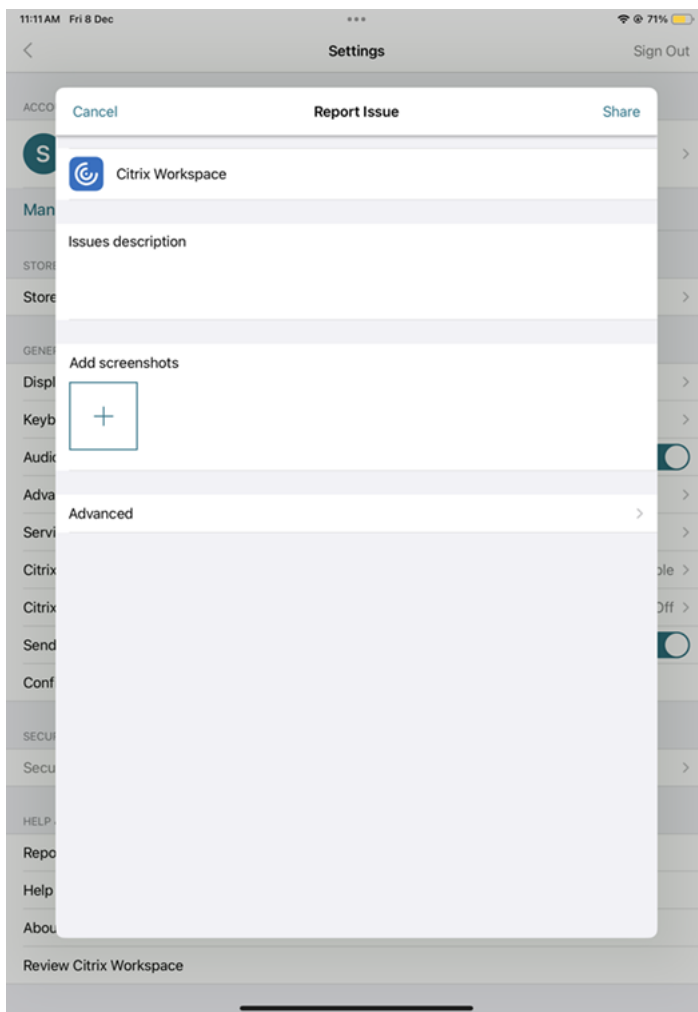
## **Cómo restablecer la aplicación Citrix Workspace**

Puede restablecer la aplicación Citrix Workspace mediante uno de los siguientes métodos:

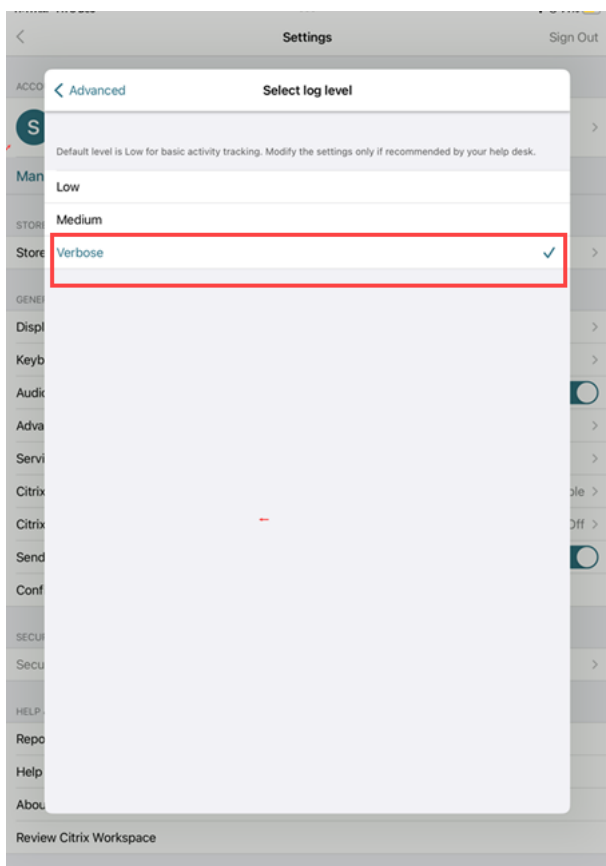
- Elimine todas las cuentas existentes de la aplicación Citrix Workspace
- Borre los datos de almacenamiento de la aplicación Citrix Workspace
- Desinstale la aplicación Citrix Workspace e instale la aplicación Citrix Workspace para iOS más reciente que tenga las correcciones más actualizadas.

## **Cómo recopilar registros**

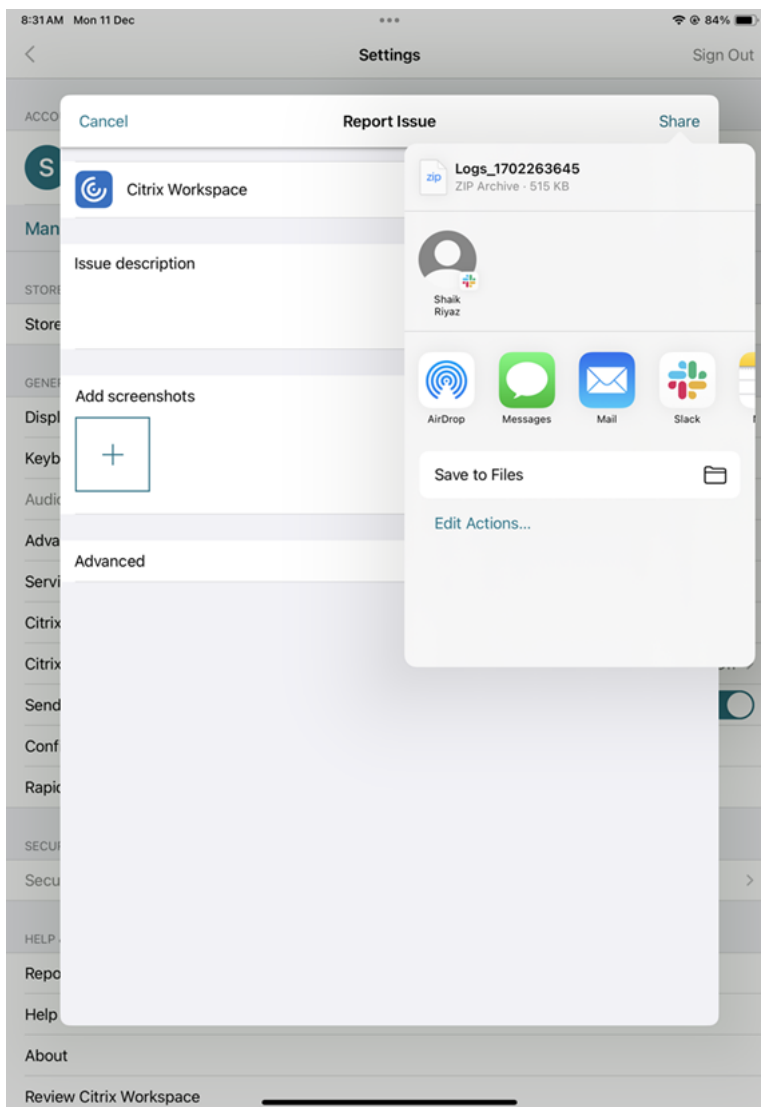
1. Abra la aplicación Citrix Workspace y vaya a **Parámetros**.
2. En **Ayuda y soporte**, seleccione **Notificar problema**.



3. Reproduzca su problema.
4. En la página Seleccionar nivel de registro, seleccione **Detallado**.



5. En la página **Seleccionar ubicación del registro**, seleccione **Consola y archivo**.
6. Comparta el archivo zip con Citrix.



### Cómo solicitar mejoras

Puede enviar sus solicitudes de mejoras mediante [este formulario](#).

### Cómo acceder a las funciones en Technical Preview

Puede solicitar funciones de la Technical Preview mediante un formulario de Podio que es único para cada función. Encontrará este formulario adjunto al anuncio de la Technical Preview en la [Documentación del producto](#).

## Cómo enviar comentarios sobre EAR

Para enviar comentarios sobre la versión de EAR, toque [aquí](#).

## Problemas comunes y consejos para solucionar problemas

### Sesiones desconectadas

Los usuarios pueden desconectarse (no cerrar la sesión) de una sesión de la aplicación Citrix Workspace para iOS mediante los siguientes métodos:

- Mientras está viendo una aplicación publicada o un escritorio en una sesión:
  - Toque la flecha en la parte superior de la pantalla para ver el menú desplegable de la sesión.
  - Toque el botón **Inicio** para volver a la pantalla de inicio.
  - Observe la sombra blanca debajo del icono de una de las aplicaciones publicadas que aún están en una sesión activa; toque el icono.
  - Toque Desconectar.
- Cierre la aplicación Citrix Workspace para iOS.
  - Toque dos veces seguidas el botón **Inicio** del dispositivo.
  - Busque la aplicación Citrix Workspace para iOS en la vista del Selector de app de iOS.
  - Toque Desconectar en el cuadro de diálogo que aparece.
- Presione el botón de inicio del dispositivo móvil.
- Toque Inicio o Cambiar en el menú desplegable de la aplicación.

La sesión permanece en estado desconectado. Si bien el usuario puede reconectarse más tarde, puede verificar que las sesiones desconectadas se muestren como inactivas transcurrido un tiempo específico.

Para mostrar la aplicación en modo inactivo, configure un tiempo de espera de sesión para la conexión ICA-TCP en Configuración de host de sesión de Escritorio remoto (antes denominada “Configuración de servicios de Terminal Server”).

Para obtener más información sobre la configuración de Servicios de Escritorio remoto (anteriormente “Servicios de Terminal Server”), consulte la documentación de Microsoft Windows Server.

### Contraseñas caducadas

La aplicación Citrix Workspace para iOS admite el cambio de las contraseñas caducadas por parte de los usuarios. Se les solicitará que introduzcan la información requerida.

## Dispositivos liberados por jailbreak

Los usuarios pueden poner en peligro la seguridad de la implementación si se conectan con dispositivos iOS liberados por jailbreak. Los dispositivos liberados por jailbreak son aquellos dispositivos que han sido modificados por sus usuarios, normalmente para evitar ciertas medidas de protección de la seguridad.

Cuando la aplicación Citrix Workspace para iOS detecta un dispositivo iOS liberado por jailbreak, muestra una alerta al usuario.

Para ayudar a proteger mejor la seguridad de su entorno, puede configurar StoreFront o la Interfaz Web para intentar impedir la ejecución de sus aplicaciones desde dispositivos liberados por jailbreak detectados.

### Requisitos

- Citrix Receiver para iOS 6.1 o versiones posteriores
- StoreFront 3.0 o Interfaz Web 5.4 o versiones posteriores
- Acceso a StoreFront o a la Interfaz Web con una cuenta de administrador

### Para impedir que los dispositivos liberados por jailbreak detectados puedan ejecutar aplicaciones

1. Inicie sesión en el servidor StoreFront o el servidor de Interfaz Web como usuario con privilegios de administrador.
2. Busque el archivo **default.ica**, que se encuentra en alguna de estas ubicaciones:
  - `C:\inetpub\wwwroot\Citrix\*storename*\conf` (Microsoft Internet Information Services)
  - `C:\inetpub\wwwroot\Citrix\*storename*\App\_Data` (Microsoft Internet Information Services)
  - `./usr/local/tomcat/webapps/Citrix/XenApp/WEB-INF` (Apache Tomcat)
3. En la sección **[Application]**, agregue: **AllowJailBrokenDevices=OFF**
4. Guarde el archivo y reinicie el servidor StoreFront o el servidor de Interfaz Web.

Una vez reiniciado el servidor de StoreFront, los usuarios que vean la alerta sobre dispositivos liberados por jailbreak ya no podrán iniciar aplicaciones desde el servidor de StoreFront o el servidor de Interfaz Web.

**Para permitir que los dispositivos liberados por jailbreak detectados ejecuten aplicaciones** Si no configura el parámetro AllowJailBrokenDevices, el comportamiento predeterminado es mostrar la

alerta a los usuarios de dispositivos liberados por jailbreak, pero permitirles iniciar aplicaciones de todos modos.

Si quiere permitir explícitamente que los usuarios ejecuten aplicaciones desde dispositivos liberados por jailbreak:

1. Inicie sesión en el servidor StoreFront o el servidor de Interfaz Web como usuario con privilegios de administrador.
2. Busque el archivo default.ica, que se encuentra en alguna de estas ubicaciones:
  - `C:\inetpub\wwwroot\Citrix\*storename*\conf` (Microsoft Internet Information Services)
  - `C:\inetpub\wwwroot\Citrix\*storename*\App\_Data` (Microsoft Internet Information Services)
  - `./usr/local/tomcat/webapps/Citrix/XenApp/WEB-INF` (Apache Tomcat)
3. En la sección **[Application]**, agregue: **AllowJailBrokenDevices=ON**
4. Guarde el archivo y reinicie el servidor StoreFront o el servidor de Interfaz Web.

Cuando el parámetro AllowJailBrokenDevices se ha configurado con el valor ON, los usuarios ven la alerta de uso de dispositivos liberados por jailbreak, pero pueden ejecutar aplicaciones desde StoreFront o la Interfaz Web.

### **Pérdida de la calidad de sonido HDX**

Desde Citrix Virtual Apps and Desktops y Citrix DaaS (antes denominado Citrix Virtual Apps and Desktops Service), es posible que se pierda calidad del sonido HDX enviado a la aplicación Citrix Workspace para iOS. Este problema se produce cuando se utilizan audio y vídeo simultáneamente.

Este problema ocurre cuando las directivas HDX de Citrix Virtual Apps and Desktops y Citrix DaaS no pueden gestionar la cantidad de información de sonido y vídeo.

Para obtener información sobre cómo crear directivas para mejorar la calidad de sonido, consulte el artículo [CTX123543](#) de Knowledge Center.

### **Error al iniciar las sesiones de escritorios y aplicaciones para una experiencia de almacén personalizado**

Es posible que no pueda iniciar sesiones de escritorios y aplicaciones desde la aplicación Citrix Workspace si tiene una experiencia de almacén personalizado. La detección automática del tipo de almacén solo se admite para direcciones de correo electrónico y no para las URL de almacén. Si tiene

un almacén personalizado, se recomienda usar la dirección de correo electrónico o el modo de inicio de sesión desde la interfaz web. Para obtener más información, consulte [Configuración manual](#) y [Configurar la detección de cuentas basada en direcciones de correo electrónico](#).

Para configurar una cuenta manualmente mediante el modo de inicio de sesión en la interfaz web, siga estos pasos:

1. Toque el **icono Cuentas > pantalla Cuentas > signo más (+)**. Se muestra la pantalla **Nueva cuenta**.
2. En la parte inferior izquierda de la pantalla, toque el icono a la izquierda de **Opciones** y luego en **Configuración manual**. Aparecerán otros campos en la pantalla.
3. En el campo **Dirección**, introduzca la dirección URL segura del sitio o Citrix Gateway (por ejemplo, agee.miEmpresa.com).
4. Seleccione la conexión **Interfaz Web**. Este modo de conexión muestra un sitio web de Citrix Virtual Apps similar a un explorador web. Esta interfaz de usuario se conoce como vista web.



1:50 PM Tue 19 Mar 37%

[Cancel](#) **New Account** [Save](#)

---

**Address** `https://ag.cldblr.com`

---

**Description** WI Store

---

**Auto-Configure**

---

**Web Interface**

---

**XenApp Services**

---

**Access Gateway**

---

**Ignore certificate warnings**

[Help & Support](#)

5. Para el certificado de seguridad, use el parámetro del campo **Ignorar advertencias de certificados** para determinar si quiere conectar con el servidor, aunque este tenga un certificado no válido, autofirmado o caducado. De forma predeterminada, está desactivado.

**Importante:**

Si habilita esta opción, compruebe que se conecta al servidor correcto. Citrix recomienda encarecidamente que todos los servidores tengan un certificado válido para proteger a los dispositivos de usuario contra posibles ataques a la seguridad. Un servidor seguro usa un certificado SSL emitido por una entidad de certificación. Citrix no admite certificados autofirmados y no recomienda ignorar la seguridad de certificados.

6. Toque **Guardar**.
7. Introduzca su nombre de usuario y su contraseña (o token, si seleccionó la autenticación de dos factores), y toque Inicio de sesión. Aparecerá la pantalla de la aplicación Citrix Workspace para iOS, desde la cual puede acceder a sus escritorios, así como agregar y abrir aplicaciones.

**Nota:**

Debe introducir las credenciales de usuario para cada conexión, ya que no se guardan en el modo de inicio de sesión de interfaz web.

## Preguntas frecuentes

### Cómo mejorar el rendimiento del vídeo en aplicaciones virtuales y escritorios virtuales para dispositivos móviles o de bajo consumo

Para obtener información sobre cómo mejorar y configurar el rendimiento del vídeo de los escritorios virtuales mediante el valor de Registro MaxFramesPerSecond o mediante directivas HDX, en función de la versión de Citrix Virtual Apps and Desktops, consulte el artículo [CTX123543](#) de Knowledge Center.

### No puedo ver mis aplicaciones o escritorios después de iniciar sesión en la aplicación Citrix Workspace

Contacte con el servicio de asistencia de su empresa o con el administrador del equipo de asistencia técnica de TI para obtener más ayuda.

### ¿Cómo solucionar problemas de conexiones lentas?

Si tiene alguno de los siguientes problemas, siga los pasos que se mencionan en la sección **Solución temporal** a continuación.

- Conexiones lentas al sitio de Citrix Virtual Apps and Desktops
- Faltan iconos de aplicaciones
- Mensajes recurrentes del tipo Error de controlador de protocolo

**Solución temporal** Inhabilite las propiedades del adaptador Ethernet Citrix PV para la interfaz de red del servidor Citrix Virtual Apps, Citrix Secure Web Gateway y el servidor de Interfaz Web.

Las propiedades del adaptador Citrix PV Ethernet incluyen las siguientes propiedades que están habilitadas de forma predeterminada. Debe inhabilitar todas estas propiedades.

- Large Send Offload
- Offload IP Checksum
- Offload TCP Checksum
- Offload UDP Checksum

**Nota:**

No es necesario reiniciar el servidor. Esta solución temporal se aplica a Windows Server 2003 y 2008 de 32 bits. Este problema no afecta a Windows Server 2008 R2.

### **Solucionar problemas con las teclas numéricas y los caracteres especiales**

Si las teclas numéricas o los caracteres del IME chinos no funcionan según lo esperado, deberá inhabilitar la opción Teclado Unicode.

Para inhabilitar la opción de teclado Unicode:

1. Vaya a **Parámetros > Opciones de teclado**.
2. Establezca **Usar teclado Unicode** en **Desactivado**.

## **Aplicación Citrix Workspace para iOS**

July 1, 2024

El software de cliente de la aplicación Citrix Workspace para iOS está disponible para su descarga desde el App Store. Le permite acceder a aplicaciones y ejecutar escritorios alojados, entregados por Citrix Virtual Apps and Desktops.

iOS es el sistema operativo de los dispositivos móviles de Apple, como iPads y iPhones. La aplicación Citrix Workspace para iOS se ejecuta en dispositivos que usan el sistema operativo iOS, por ejemplo iPhone X, iPad mini y iPad Pro.

### **Idiomas disponibles**

La aplicación Citrix Workspace para iOS está adaptada para usarse en otros idiomas que no son el inglés. Para obtener una lista de los idiomas disponibles en la aplicación Citrix Workspace para iOS, consulte [Idiomas disponibles](#).

## Elementos retirados

El anuncio de este artículo ofrece un adelanto de las plataformas, los productos y las funciones de Citrix que se están retirando progresivamente, de modo que pueda tomar a tiempo las decisiones empresariales pertinentes. Citrix analiza el uso que hacen los clientes de una función que está por retirar y los comentarios que tengan sobre la eliminación de la función para determinar cuándo retirarla. Estos anuncios están sujetos a cambios en las versiones posteriores y es posible que no contengan todas las funciones o funciones retiradas.

Los elementos retirados no se quitan inmediatamente. Citrix sigue dándoles asistencia en esta versión, pero en el futuro se retirarán.

| Elemento                                            | Retirada anunciada en                                      | Eliminado en                                           | Alternativa                                                                                                                    |
|-----------------------------------------------------|------------------------------------------------------------|--------------------------------------------------------|--------------------------------------------------------------------------------------------------------------------------------|
| Compatible con el protocolo DTLS 1.0                | Versión 24.5.0 de la aplicación Citrix Workspace para iOS  | -                                                      | Protocolo DTLS 1.2                                                                                                             |
| Compatibilidad con los protocolos TLS 1.0 y TLS 1.1 | Versión 24.4.0 de la aplicación Citrix Workspace para iOS  | -                                                      | Protocolo TLS 1.2 o TLS 1.3                                                                                                    |
| Servicios XenApp (también conocidos como PNAgent)   | Versión 23.7.5 de la aplicación Citrix Workspace para iOS  | -                                                      | En la aplicación Citrix Workspace, conéctese a los almacenes con la URL de almacén en lugar de la URL de los servicios XenApp. |
| Versión 14 del sistema operativo iOS                | Versión 23.10.0 de la aplicación Citrix Workspace para iOS | Objetivo: Aplicación Citrix Workspace para iOS 23.12.0 | Actualizar iOS a la versión disponible más reciente                                                                            |
| Versión 13.x del sistema operativo iOS              | Versión 22.9.5 de la aplicación Citrix Workspace para iOS  | Objetivo: Diciembre de 2022 y versión 22.12.0          | Actualizar iOS a la versión disponible más reciente                                                                            |
| Versiones 11.x y 12.x del sistema operativo iOS     | Versión 21.12.0 de la aplicación Citrix Workspace para iOS | Objetivo: Agosto de 2022 y versión 22.8.0              | Actualizar iOS a la versión disponible más reciente                                                                            |
| Versión 10.x del sistema operativo iOS              | Versión 21.1.5 de la aplicación Citrix Workspace para iOS  | La versión posterior a 21.1.5                          | Usar la versión 21.1.5 de la aplicación Citrix Workspace para iOS o una anterior                                               |

**Notas:**

- Los usuarios existentes de la aplicación Citrix Workspace en versiones de plataforma obsoletas no pueden actualizar la aplicación Citrix Workspace a la versión más reciente (del App Store).
- Los nuevos usuarios de la aplicación Citrix Workspace en versiones de plataforma obsoletas solo pueden descargar una versión anterior compatible del App Store.
- Los usuarios de las versiones de plataforma obsoletas no reciben ni las funciones ni los parches de seguridad nuevos que vienen con cada versión más reciente de la aplicación Citrix Workspace.



© 2024 Cloud Software Group, Inc. All rights reserved. Cloud Software Group, the Cloud Software Group logo, and other marks appearing herein are property of Cloud Software Group, Inc. and/or one or more of its subsidiaries, and may be registered with the U.S. Patent and Trademark Office and in other countries. All other marks are the property of their respective owner(s).